(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10177525 A**

(43) Date of publication of application: **30 . 06 . 98**

(51) Int. Cl **G06F 12/14**
G08B 25/10
H04Q 7/38

(21) Application number: **08335336**

(22) Date of filing: **16 . 12 . 96**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

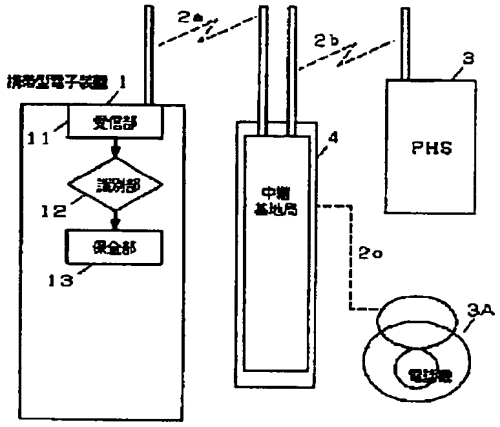
(72) Inventor: **MIURA FUSAKI**

(54) PROTECTIVE SYSTEM FOR PORTABLE ELECTRONIC DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent the owner of a stolen or lost portable electronic device or a called subscriber from suffering damage.

SOLUTION: A portable electronic device 1 is provided with a receiving section 11 which receives remote control data transmitted through a radio communication means, a discriminating section 12 which discriminates the received remote control data, and a prescribed security section 13 which prevents the owner of the electronic device 1 from suffering from damage based on the discriminated result of the discriminating section 12. Therefore, when the electronic device 1 is stolen or lost, the security of the property or information of the owner of the electronic device can be improved, because the security section 13 performs security processing before the owner takes the necessary procedure to the line undertaking company of a network or on-line system for canceling the contract on his line.



COPYRIGHT: (C)1998,JPO

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－177525

(43)公開日　平成10年(1998)６月30日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｄ
Ｇ０８Ｂ　25/10		Ｇ０８Ｂ　25/10	Ｚ
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ

審査請求　未請求　請求項の数19　ＯＬ　（全 26 頁）

(21)出願番号　特願平8－335336

(22)出願日　平成８年(1996)12月16日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　三浦　興己
神奈川県横浜市港北区網島東四丁目３番１号　松下通信工業株式会社内

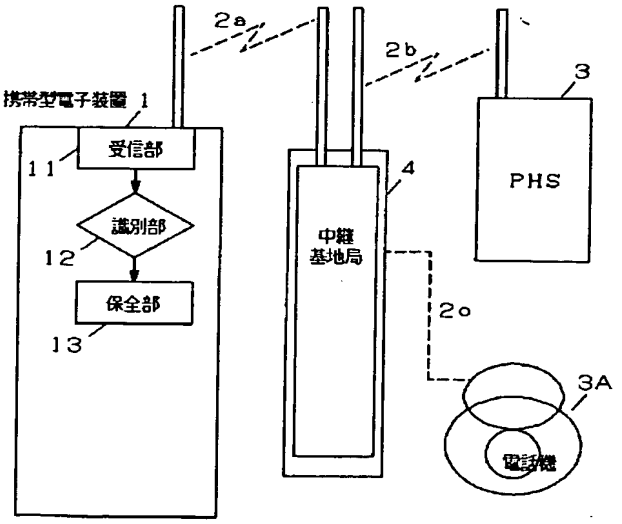
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】　携帯型電子装置の保全システム

(57)【要約】

【課題】　盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除する。

【解決手段】　携帯型電子装置１に電波通信手段を介して送信されてくる遠隔操作データを受信する受信部１１と、受信部１１で受信した遠隔操作データを識別する識別部１２と、識別部１２による識別結果に基づいて携帯型電子装置１の所有者が害を被ることを排除する所定の保全部１３を設け、携帯型電子装置１が盗まれたり紛失した場合に、ネットワークやオンラインシステムの回線事業会社に連絡して回線の解約解除の手続きをする前に、保全部１３で保全処理することにより、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを可能にする。



1

【特許請求の範囲】

【請求項１】　携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設け、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを特徴とする携帯型電子装置の保全システム。

【請求項２】　携帯型電子装置が盗まれたり紛失した時に電波通信手段を介して送信されてきた遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたことを特徴とする請求項１記載の携帯型電子装置の保全システム。

【請求項３】　電波通信手段を介して送信されてくる遠隔操作データ受信し、該遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を１つまたは１つ以上設けたことを特徴とする請求項２記載の携帯型電子装置の保全システム。

【請求項４】　保全処理手段は、携帯型電子装置の所有者が予め入力したキーワードを記憶する第１記憶手段と、電波通信手段を介して送信される遠隔操作データを受信し、該遠隔操作データの識別結果のキーワード情報を記録する第２記録手段、前記第１記憶手段のキーワードと前記第２記録手段のキーワード情報との一致を確認した後、保全処理を実行することを特徴とする請求項２または３記載の携帯型電子装置の保全システム。

【請求項５】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項６】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項７】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に記憶した連絡先やメッセージを表示し、携帯型電子装置を回収する「メッセージ表示」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項８】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に記憶した連絡先にのみ交信する「所有者連絡発信」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

2

【請求項９】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の本来の機能のうち所有者が予め入力した機能を停止する「発信機能禁止」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１０】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１１】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを消去し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１２】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１３】　保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１４】　保全処理手段の保全処理内容として、使用者の識別手段により使用者を識別し、所有者以外の他人が携帯型電子装置の使用を不可能にする「保全処理」を行うことを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１５】　送信した相手または相手情報に対する保全処理手段は、遠隔操作データによって、

ａ．携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理と、

ｂ．携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理と、

ｃ．携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理と、

ｄ．携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理と、

ｅ．携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセージを送信する保全処理と、

ｆ．携帯型電子装置に送信した相手に、該携帯型電子装置の保全システムの使用を防止する保全処理と、のうち１つ以上の処理を実施することを特徴とする請求項３記載の携帯型電子装置の保全システム。

【請求項１６】　電波通信手段を伝送媒体にして、所有者が予め入力して記憶手段に記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全処理手段を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことを特徴とする請求項５乃至１４の何れかに記載の携帯型電子装置の保全システム。

【請求項１７】　所有者が予め入力して記憶手段に記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置を接続し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことを特徴とする請求項５乃至１４の何れか１項に記載の携帯型電子装置の保全システム。

【請求項１８】　携帯型電子装置に保全処理を促すための発振手段、該発振手段の発振信号を送信する微弱電力送信手段を有する携帯型電子装置の子機と、該子機からの保全処理を促すための発振データを受信する微弱電力受信手段、該微弱電力受信手段で受信した操作データを識別する識別手段、該識別手段の識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を揺する本体を備え、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることを特徴とする携帯型電子装置の保全システム。

【請求項１９】　携帯型電子装置との間で交信する微弱電力伝送手段、該微弱電力伝送手段の受信信号から携帯型電子装置との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を促すための発振データを前記微弱電力伝送手段で受信し、該発振データにより警告音を発生する手段を有する携帯型電子装置の子機と、前記子機と同様の双方の微弱電力伝送手段、子機との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を起動し、警告音を発生する手段を有する本体を備え、紛失あるいは盗難および置き忘れを防止することを特徴とする携帯型電子装置の保全システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯型電子装置（ＰＨＳ、携帯電話機も含む電波通信手段を有するデータ処理端末装置をいう）の盗難や紛失に対して所有者が害を被ることを排除し、所定のセキュリティを高める保全処理機能を備えた携帯型電子装置の保全システムに関する。

【０００２】

【従来の技術】従来、上記のような携帯型電子装置は、その装置の特色上、広い不特定領域の屋外に持ち出して使用される。また、通信回線を登録した携帯型電子装置は、ＰＨＳ（Personal Hanndy Phone System）、そのデータ処理端末装置などデジタル信号情報のコンピュータ周辺端末装置として用途が拡大するとともに、その持ち出し使用領域を広げていくことができる。また、その使用方法も容易で、多くの人々の需要がある。

【０００３】

【発明が解決しようとする課題】しかしながら、この種従来の携帯型電子装置は、所有者がその装置自体を屋外などに持ち出して使用したり、手軽に携帯できるため、盗難や紛失する機会が多く、盗難や紛失したこの種の携帯型電子装置を他人が拾得した場合にも、容易に使用できる可能性があり、元々の所有者はプライベイト情報や重要データを盗み見されたり、使用していない通話料金などの請求を請けるなど所有者が害を被る問題が発生している。

【０００４】また、盗難や紛失した携帯型電子装置の所有者に送信した相手にとっても、不適切な状況であることを知らずに携帯型電子装置の所有者と思って送信したことで、送信相手または相手情報が害を被る問題が発生するおそれもある。

【０００５】本発明は、このような従来の問題点を解決するものであり、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除できる携帯型電子装置の保全システムを提供することを目的とするものである。

【０００６】

【課題を解決するための手段】この課題を解決するために本発明は、携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設けたものである。

【０００７】これにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除できる。

【０００８】

【発明の実施の形態】本発明の請求項１に記載の発明は、携帯型電子装置に電波通信手段を介して送信されてくる遠隔操作データを受信する受信手段と、前記受信手段で受信した遠隔操作データを識別する識別手段と、前記識別手段による識別結果に基づいて携帯型電子装置の所有者が害を被ることを排除する所定の保全処理手段を設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能になる。

【０００９】本発明の請求項２に記載の発明は、携帯型電子装置が盗まれたり紛失した時に電波通信手段を介して送信されてきた遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手

者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能となる。

【００１０】本発明の請求項３に記載の発明は、電波通信手段を介して送信されてくる遠隔操作データ受信し、該遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を１つまたは１つ以上設けることにより、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることが可能となる。

【００１１】本発明の請求項４に記載の発明は、保全処理手段が、携帯型電子装置の所有者が予め入力したキーワードを記憶する第１記憶手段と、電波通信手段を介して送信される遠隔操作データを受信し、該遠隔操作データの識別結果のキーワード情報を記録する第２記録手段、前記第１記憶手段のキーワードと前記第２記録手段のキーワード情報との一致を確認した後、保全処理を実行することにより、携帯型電子装置を使用する折に、個々のキーワードを入力しなければ動作せず、所有者の大切な登録情報を保全・安全・確実を保証するセキュリティが保たれ、個別のキーワードの適用により厳格に守る仕組みが成り立ち、盗難や紛失での管理作業での誤りを生ずることが回避でき、登録情報やその管理のセキュリティを高めることができる。

【００１２】本発明の請求項５に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理を行うことにより、電源が入らなくなるので携帯型電子装置の基本機能を殺す保全処理がなされ、携帯型電子装置の紛失者にとって最小限の損失に抑えることができる。

【００１３】本発明の請求項６に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理を行うことにより、携帯型電子装置の拾得者に警告発生することで携帯型電子装置の使用を禁止する保全処理が可能になり、携帯型電子装置の紛失者にとって他人に使用することを防止できる。

【００１４】本発明の請求項７に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に記憶した連絡先やメッセージを表示し、携帯型電子装置を回収する「メッセージ表示」の保全処理を行うことにより、携帯型電子装置の拾得者にメッセージ表示するから、携帯型電子装置の返却を訴える保全処理が可能になり、携帯型電子装置の紛失者にとって他人に使用することを防止でき、携帯型電子装置の返却が可能になる。

【００１５】本発明の請求項８に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に記憶した連絡先にのみ交信する「所有者連絡発信」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し所有者連絡発信で連絡が取れるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、携帯型電子装置の返却が可能になる。

【００１６】本発明の請求項９に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の本来の機能のうち所有者が予め入力した機能を停止する「発信機能禁止」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し発信機能禁止ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【００１７】本発明の請求項１０に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を保護するデータ出力禁止がかかるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【００１８】本発明の請求項１１に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを消去し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を保護する記憶データ消去ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できるほか、個人データや情報を悪用されるこを阻止できる。

【００１９】本発明の請求項１２に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理を行うことにより、携帯型電子装置の拾得者の使用に対し通信回線番号消滅ができるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避することができる。

【００２０】本発明の請求項１３に記載の発明は、保全処理手段の保全処理内容として、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理を行うことにより、携帯型電子装置内の個人データや情報を遠隔操作でデータ転送できるから、携帯型電

子装置内の個人データや情報を回収でき、携帯型電子装置内の記憶データを消去できるから、携帯型電子装置の紛失者にとって他人に使用することを防止でき、不当な使用による料金が生じるのを回避できる。

【００２１】本発明の請求項１４に記載の発明は、保全処理手段の保全処理内容として、使用者の識別手段により使用者を識別し、所有者以外の他人が携帯型電子装置の使用を不可能にする「保全処理」を行うことにより、携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることを排除する所定のセキュリティを高め得る。

【００２２】本発明の請求項１５に記載の発明は、送信した相手または相手情報に対する保全処理手段は、遠隔操作データによって、ａ．携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理と、ｂ．携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理と、ｃ．携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理と、ｄ．携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理と、ｅ．携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセージを送信する保全処理と、ｆ．携帯型電子装置に送信した相手に、該携帯型電子装置の保全システムの使用を防止する保全処理のうち１つ以上の処理を実施することにより、携帯型電子装置が盗難や紛失された場合には、携帯型電子装置の保全システムの所有者が予め入力したキーワードを蓄積記憶させておき、電波通信を媒体にし遠隔操作でそのキーワードデータを他の電送装置から送信すると、キーワード情報との一致を確認した後で、保全処理を実行することができ、所有者の大切な登録情報を保全・安全・確実を保証するセキュリティが保たれるものであり、盗難や紛失しても他人に悪用される危険を回避できる。

【００２３】本発明の請求項１６に記載の発明は、電波通信手段を伝送媒体にして、所有者が予め入力して記憶手段に記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全処理手段を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことにより、携帯型電子装置の紛失者が予め入力して記憶手段に蓄積記憶したキーワード信号を送信し、強制的に携帯型電子装置の保全機能を駆動し、装置の紛失者にとって他人に使用されることを防止できる。

【００２４】本発明の請求項１７に記載の発明は、所有者が予め入力して記憶手段に記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置を接続し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理を行うことにより、携帯型電子装置の拾得者が応答しなとか、交信ができない事態の場合においても、呼び出し信号回数のパターンによる遠隔保全処理を起動させ、装置の紛失者にとって他人に使用されることを防止できる。

【００２５】本発明の請求項１８に記載の発明は、携帯型電子装置に保全処理を促すための発振手段、該発振手段の発振信号を送信する微弱電力送信手段を有する携帯型電子装置の子機と、該子機からの保全処理を促すための発振データを受信する微弱電力受信手段、該微弱電力受信手段で受信した操作データを識別する識別手段、該識別手段の識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を揺する本体を備えることにより、未然に紛失または置き忘れを防止し回避することができ、また所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【００２６】本発明の請求項１９に記載の発明は、携帯型電子装置との間で交信する微弱電力伝送手段、該微弱電力伝送手段の受信信号から携帯型電子装置との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を促すための発振データを前記微弱電力伝送手段で受信し、該発振データにより警告音を発生する手段を有する携帯型電子装置の子機と、前記子機と同様の双方の微弱電力伝送手段、子機との間の距離を判別する判別手段、該判別手段による所定の距離より離れた判別結果により保全処理を起動し、警告音を発生する手段を有する本体を備えることにより、携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置の保全システムを容易に実施することができ、携帯型電子装置を紛失または置き忘れを防止できる。

【００２７】以下、本発明の実施の形態について、図面を参照して説明する。

（実施の形態１）図１は、本発明の請求項１に対応する実施の形態１における携帯型電子装置の保全システムの構成図である。同図において、１は例えばＰＨＳ（Personal Handy Phone System）データ通信装置や携帯電話としての携帯型電子装置、２ａ，２ｂ，２ｃは公衆回線網などに接続された通信回線などの電波通信手段、３は公衆回線網などに接続された一般公衆電話や携帯電話としてのＰＨＳなど電話機、４は中継基地局である。更に電話機３Ａは公衆回線網などに接続された中継基地局４から無線通信回線２ｂを介した別のＰＨＳデータ通信装置や携帯電話としてのＰＨＳを構成する。

【００２８】携帯型電子装置１は、電波通信手段２ａを伝送媒体にし遠隔操作データを受信する受信部１１、受信した遠隔操作データを識別する識別部１２、この識別部１２の識別結果により携帯型電子装置１の所有者が害

を被ることを排除する所定の保全部１３を備え、携帯型電子装置１の所有者の財産または情報に関わるセキュリティを行い、携帯型電子装置所有者の財産または情報を保全する。

【００２９】市内や市外の一般公衆電話３から公衆回線網２ｂを介して、またＰＨＳデータ通信装置や携帯電話としてのＰＨＳ３Ａから無線通信回線２ｃを介して保全を要する携帯型電子装置１に遠隔操作データを送信する。該携帯型電子装置１は該遠隔操作データを受信部１１で受信し、受信した遠隔操作データが予め記憶された所定の遠隔操作データと一致したかを識別部１２が判別する。識別部１２では、その識別結果により一致が確認された場合のみ保全部１３が携帯型電子装置１の所有者が害を被ることを排除するために所定の保全処理を行う。

【００３０】次に、図４は携帯型電子装置のネットワークシステムを示す構成図であり、公衆ならびに専用回線網３０には、交換機を介して一般の電話機３１が接続されているとともに、変復調器（MODEM)付きのパソコン３２、携帯型電子装置の多数の基地局３３～３５および網管理局３６が接続される。多数の基地局３３～３５には個々の携帯型電子装置が無線通信回線を介し接続される。例えば、基地局３３には無線通信回線を介して携帯型パソコン、無線通信パソコン、無線通信電子手帳が接続され、基地局３４は無線通信回線を介して携帯型電話機、ＰＨＳ、目線通信機が接続され、基地局３５は無線通信回線を介して携帯型情報端末機が接続されている。また、網管理局３６は網全体を制御し管理するもので、各端末に対しての制御を行なう。

【００３１】個々の携帯型電子装置は保全機能を備えており、この保全機能は、その所有者より送信された遠隔操作データを受信した場合、この遠隔操作データに基づいて携帯型電子装置の所有者に不利益になる要因を排除する所定の保全処理を実行するための制御や、キーワードの入力や解析処理を実施するための制御を行ない、また異なった入力に対しても設定された保全処理を実施するための制御を行う。

【００３２】したがって、本発明の実施の形態１では、携帯型電子装置は電波通信手段と伝送媒体を通して遠隔操作データを受信部１１、受信した遠隔操作データを識別する識別部１２、この識別部１２の識別結果により携帯型電子装置の所有者が害を被ることを排除する保全部１３により、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることができるという効果がある。

【００３３】（実施の形態２）図２は、本発明の請求項２に対応する実施の形態２における携帯型電子装置の保全システムの構成を示す、例えばＰＨＳ端末の機能ブロック図であり、キー基板とＲＦ基板で構成される。同図において、モデム部２２１は、音声符号をの適応予測と適応量子化により圧縮／伸張するＡＤＰＣＭコーディック２２１１、バッファー２２１２、フレームプロセッサ２２１３、π/4ＱＰＳＫ変調器２２１４及びπ/4ＱＰＳＫ復調器２２１５を備え、ＡＤＰＣＭコーディック２２１１にはＰＣＭコーディック２２８を介してスピーカ２３３及びマイク２３４が接続されている。また、２３５はバッテリ、２３６は電圧安定器、２３７は各回路へ電源を供給する電源回路である。

【００３４】プロトコール・プロセッサ部２３０は、所定のプロトコールに従い携帯型電子装置を制御するもので、ＣＰＵとメモリ等から構成される。図３はプロトコール・プロセッサ部の構成を示している。同図において、プロトコール・プロセッサ部２３０は、ＣＰＵ（制御部）２３０１、プロトコール・プロセッサ２３０２、カレンダ時計，タッチパネル，表示部Ｉ／Ｆ，赤外線Ｉ／Ｆ，シリアルＩ／Ｆ，ＰＣカードＩ／Ｆ，音声発生Ｉ／Ｆ，各種センサＩ／Ｆ，各種入力Ｉ／Ｆ等に対するマンマシンＩ／Ｆプロセッサ２３０３、ＲＡＭ，ＲＯＭ，Ｆ－ＲＯＭの相当するメモリ２３０４、保全処理部２３０５、発信機能，送信機能，転送機能を発揮するプロトコルプロセッサ２３０６、ＲＦコントローラ２３０７及び電源制御部２３０８を備え、マンマシンＩ／Ｆプロセッサ２３０３にはキーパット２３１及びＬＣＤドライブ２３２が接続されている。

【００３５】この構成において、無線送受信部はアンテナ２０１に到来する電波を受信側に選択された送受信切替用のＦＥＴスイッチ２０２を経由し、受信帯域のバンドパスフィルタ（ＢＰＦ）２０３で選択された後、ＬＮＡ（ローノイズアンプ）２０４で増幅される。このＬＮＡ２０４にはアッテネータが内蔵され、強電界での信号入力時にはアッテネータに切り換えることによって受信回路の飽和を防ぎ広いダイナミックレンジを確保する。ＬＮＡ２０４で増幅された信号は、送受信切替用のＦＥＴスイッチ２０５を介して、もう１段のバンドパスフィルタ（ＢＰＦ）２０６に送出され、このＢＰＦ２０６でイメージなどの不要電波を除去した後、送受信切替用のＦＥＴスイッチ２０７を介して第１ミキサ２０８へ送られる。

【００３６】第１ミキサ２０８では、受信信号と、発振部（ＴＣＸＯ）の発振信号を基にシンセサイザ２１０からアンプ２１１を通して得られる第１ローカル信号とをミキシングし、周波数チャネルの選択を行なうとともに248.45ＭＨｚの中間周波数へ変換する。このミキサ２０８は相互変調による耐妨害特性を高めるため、高いインターセプトポイントを有する。ミキサ２０８の出力は、送受信切替用のＦＥＴスイッチ２１２を介して狭帯域フィルタ特性のＳＡＷフィルタ（ＢＰＦ）２１３を経由して出力される。このＳＡＷフィルタ２１３は隣接チャネルの選択度およびイメージ妨害特性を決定し、同時に優れた群遅延特性を有する。ＳＡＷフィルタの代用として

アナログコードレス用のヘリカルフィルタを使用した場合は、イメージ周波数のみ減衰させ、次段の中間周波数で除去する。

【００３７】ＳＡＷフィルタ２１３を通過した信号は送受信切替用のＦＥＴスイッチ２１４を介して第２ミキサ２１５に入力され、ローカル発振器２１８からの信号とミキシングすることにより10.75 MHz に変換させる。第２イメージ妨害はＳＡＷフィルタ２１３の能力のみで決まるため、第２ミキサ２１５はイメージリジェクトタイプのものである。これによりＳＡＷフィルタ２１３のイメージ除去能力は緩和する。10.75 MHz のＩＦ信号はバンドパスフィルタ（ＢＰＦ）２１６通過した後、第３ミキサ２１７でローカル発振器２１８からの信号とミキシングされ、さらにバンドパスフィルタ（ＢＰＦ）２１９を通過させることで1.15MHｚに変換する。そして、リミッタ２２０で検出された信号はモデム部２２１に送られる。

【００３８】一方、モデム部２２１のπ/4ＱＰＳＫ変調器２２１４で作られたπ/4ＱＰＳＫ変調波は、デジタルデータとして図示省略のＤ／Ａコンバータに入力される。Ｄ／Ａコンバータでは10.75 MHz の変調波となり、バンドパスフィルタ（ＢＰＦ）２２２で不要信号が除去される。10.75 MHz のＩＦ信号は送信用ミキサ２２３に入力され、ローカル発振器２１８からの信号とミキシングすることにより248.45MHｚに変換される。この送信側のＩＦ信号は受信と共用したＳＡＷフィルタ２１３を通すことによりイメージなどの不要信号を除去した後、送受信切替用のＦＥＴスイッチ２１２及びパワー調整部２２４を介して送信用ミキサ２２５へ入力される。このミキサ２２５はシンセサイザ２１０からの第１ローカル信号とミキシングされ、送信周波数に変換する。この信号は、受信と共用する帯域通話フィルタ２０６を通してパワーアンプ２２６に入力される。このパワーアンプ２２６では必要なパワーに信号を増幅し、増幅された信号はローパスフィルタ（ＬＰＦ）２２７で高周波分が除去され、送信切替用のＦＥＴスイッチ２０２を経由してアンテナ２０１から放射される。

【００３９】一方、マイク２３４から入力された音声信号はＰＣＭコーデッィック２２８でデジタル化され、64 Kbpsで入力されるＰＣＭ信号をＡＤＰＣＭコーディック２２１１でＡＤＰＣＭ変換（圧縮）し、32Kbpsのデータにする。このデータは一旦バッファ２２１２に一時記憶させた後、フレームプロセッサ２２１３でＴＤＭＡフレームに構成する。このときにユニークワード、ＣＩ、ＳＡ、ＣＲＣ等の付加情報が加わるため、384 Kbps までデータレートは増加する。このデータをπ/4ＱＰＳＫ変調器２２１４で10.75 MHz の変波として図示省略のＤ／Ａコンバータに入力する。一方、1.15MHｚの受信データはπ/4ＱＰＳＫ復調器２２１５で検波され、ＡＤＰＣＭコーディック２２１１で64Kbpsに伸張され、ＰＣＭコーディック２２８でＤ／Ａ変換されてスピーカ２３３へ出力される。その他に、送信／受信の切り替えタイミングの制御、ＲＳＳＩの検出判定、ＡＦＣ制御やシンセサイザデータの設定、及び無線系のコントロールを行う。また、本実施の形態２の場合、遠隔操作データを受信した時には、この受信した遠隔操作データに基づき携帯型電子装置の所有者が害を被ることを排除する保全処理部２３０５を制御し、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高める保全処理を実行すべき制御を行う。

【００４０】次に、携帯型電子装置の所有者が携帯型電子装置を盗まれたり紛失した場合について述べる。この場合は、図５に示すセキュリティを高める保全処理の制御ルーチンを実行する。まず、ステップＳ１０において、携帯型電子装置の所有者は網管理局３６に対して変復調器（ＭＯＤＥＭ）を介しパソコン３２を用いて所有する携帯型電子装置に対して通信を開始すべく遠隔操作データを入力する。この場合、携帯型電子装置が携帯していない状況（盗難や紛失）および内部に記憶されている情報の重要度により送信する遠隔操作データの内容を選択する。遠隔操作データには制御コードが所有者のみが事前に付加しており、所有者のみが知っているキーワードがある。したがって、所有者以外の例えば拾得者が任意に所有者の携帯型電子装置に対して遠隔操作データを送ることや解除することはできない。これにより遠隔操作の悪用を防止できる。

【００４１】また、携帯型電子装置のネットワークシステムで、携帯型電子装置の所有者がパソコン３２を保有していないような場合、または保有していても網管理局３６に対して変復調器（ＭＯＤＥＭ）を介し駆動するシステムになっていない時は、公衆回線網３０の一般の電話機３１により携帯型電子装置の基地局３４に遠隔操作データの送信を依頼する。またはプッシュ回線により遠隔操作データを入力する。

【００４２】次のステップＳ１１では、携帯型電子装置の所有者が入力した遠隔操作データを公衆ならびに専用回線網３０を介して携帯型電子装置の基地局３４に転送する。次のステップＳ１２では、携帯型電子装置の基地局３４より無線で遠隔操作データを送信する。

【００４３】以上のようにパソコン３２より入力した遠隔操作データが公衆ならびに専用回線網３０を介して携帯型電子装置の基地局３４に送られ、目的の所有者の手元にない所有者の携帯型電子装置に送信される。なお、携帯型電子装置が双方向二重通損の機能を有しておれば、リンクが確立し所有者の操作するパソコン３２へ携帯型電子装置の受信が確実に実行されたことを伝送する。

【００４４】したがって、本実施の形態２では、電波通信手段を伝送媒体にし受信した遠隔操作データの識別結果により、携帯型電子装置の所有者が害を被ることを排

除でき、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高める得る効果がある。

【００４５】（実施の形態３）次に、携帯型電子装置の所有者がその装置を盗まれたり紛失して、該携帯型電子装置を他人が拾得した場合に発生しうる問題は、元々の所有者はプライベイト情報や重要データを盗み見されたり、使用していない通話料金などの請求を請けるなど該携帯型電子装置の所有者が害を被る問題と、盗難や紛失した携帯型電子装置の所有者に送信した相手にとっても、不適切な状況であることを知らずに携帯型電子装置の所有者と思ってに送信したことで、送信相手または相手情報が害を被る問題がある。

【００４６】したがって、請求項３に対応する本実施の形態３では、携帯型電子装置の所有者が、その携帯型電子装置を盗まれたり紛失した場合は、図５に示すセキュリティを高める保全処理の制御ルーチンを実行する。ステップＳ１０において、携帯型電子装置の所有者は網管理局３６に対して変復調器（ＭＯＤＥＭ）を介しパソコン３２を用いて所有する携帯型電子装置に対して通信を開始すべく遠隔操作データを入力する。この場合に携帯型電子装置が携帯していない状況（盗難や紛失）および内部に記憶されている情報の重要度により送信する遠隔操作データの内容を選択する。遠隔操作データには制御コードが事前に付加されており、この制御コードは所有者のみが知っているキーワードある。

【００４７】そこで、電波通信手段を伝送媒体にしてデータ受信した遠隔操作データの識別結果により、携帯型電子装置の所有者に送信した相手または相手情報が害を被ることを排除する保全処理手段を備える携帯型電子装置において、送信した相手または相手情報が害を被るのを防止するための保全処理手段では、携帯型電子装置の所有者が予め記憶手段に記憶しておいたキーワードと、電波通信手段を媒体にし遠隔操作データを受信した時の識別結果のキーワード情報との一致を確認した後に、後述する実施の形態１５で説明する各保全処理を実行する。

【００４８】すなわち、遠隔操作データによって、

ａ．携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理、

ｂ．携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理、

ｃ．携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理、

ｄ．携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理、

ｅ．携帯型電子装置に送信した相手に、所有者があらかじめ入力して記憶手段に蓄積記憶した紛失メッセイジを送信する保全処理、

ｆ．携帯型電子装置に送信した相手に、該携帯型電子装置の使用を防止する保全処理、のうち１つ以上の処理を実行する。

【００４９】したがって、本実施の形態３では、盗まれたり紛失した携帯型電子装置の所有者に送信した相手にとって、送信相手の携帯型電子装置が不適切な状況にあることを知り、保全処理することによって送信相手または相手情報が害をこうむるのを防止することができる。

【００５０】（実施の形態４）携帯型電子装置の所有者が、その携帯型電子装置を盗まれたり紛失した場合に、上記図５に示すセキュリティを高める保全処理の制御ルーチンのようにキーワードと遠隔操作データが所有者の手元にない所有者の携帯型電子装置に送信されると、該携帯型電子装置の保全処理手段は図６に示す遠隔操作データの処理ルーチンを実行する。以下、その処理ルーチンについて図６を参照して説明する。

【００５１】図６において、ステップＳ２０では、紛失の携帯型電子装置がキーワードと遠隔操作データを受信し、次のステップＳ２１において、遠隔操作のキーワードが予め所有者が記憶手段に記憶しておいたキーワードであるか否かを識別する。ここで、不一致である場合は保全処理システムを終了し、通常のモードに戻る。また、キーワードが一致した場合は保全処理システムを立ち上げ、装置のプロテクト機能を起動する。その後、遠隔操作データであるか否かを識別する。ここで、遠隔操作データでない場合は保全処理システムを終了し、通常のモードに戻る。また、遠隔操作データである場合はステップＳ２２に進み、遠隔操作データの保全内容を解析する。

【００５２】遠隔操作データは各保全処理にコードが予め定めてあり、例えば「警告発生」、「メッセイジ表示」、「所有者連絡発信」、「発信機能禁止」、「データ出力禁止」、「記憶データ消去」、「通信回線番号消滅」、「電源オフ」など、所定のコードにより分岐し、個々の保全処理ルーチンに進む。

【００５３】すなわち、ステップＳ２３では、遠隔操作データの内容が「警告発生」コードと一致すると判別した場合はステップＳ２４に進み、「警告発生」の保全処理を実行する。ステップＳ２３で不一致の場合は次の処理コードのステップＳ２５に進み、次々と一致するコードを検索して進む。その他の遠隔操作データの内容においても同様であり一致した場合には該当した保全処理を実行する。非該当のコードであれば保全処理システムを終了する又は固定の保全処理をする。

【００５４】次にステップ２５では、遠隔操作データの内容が「メッセイジ表示」コードと一致するか否かを識別し、一致した場合にはステップＳ２６に進み、「メッセイジ表示」の保全処理を実行する。ステップＳ２５で不一致の場合は次の処理コードのステップＳ２７に進む。ステップＳ２７では、遠隔操作データの内容が「発信機能禁止」コードと一致するか否かを識別し、一致し

た場合はステップＳ２８に進み、「発信機能禁止」の保全処理を実行する。ステップＳ２７で不一致の場合は次の処理コードのステップＳ２９に進む。

【００５５】ステップＳ２９では、遠隔操作データの内容が「所有者連絡発信」コードと一致するか否かを識別し、一致した場合はステップＳ３０に進み、「所有者連絡発信」の保全処理を実行する。ステップ２９で不一致の場合には次の処理コードのステップＳ３１に進む。

【００５６】次にステップＳ３１では、遠隔操作データの内容が「記憶データ消去」コードと一致するか否かを識別し、一致した場合にはステップＳ３２に進み、「記憶データ消去」の保全処理を実行する。ステップＳ３１で不一致の場合は次の処理コードのステップＳ３３に進む。ステップＳ３３では、遠隔操作データの内容が「データ出力禁止」コードと一致するか否かを識別し、一致した場合はステップＳ３４に進み、「データ出力禁止」の保全処理を実行する。ステップＳ３３で不一致の場合は次の処理コードのステップＳ３５に進む。

【００５７】ステップＳ３５では、遠隔操作データの内容が「通信回線番号消滅」コードと一致するか否かを識別し、一致した場合はステップＳ３６に進み、「通信回線番号消滅」の保全処理を実行する。ステップＳ３５で不一致の場合は次の処理コードのステップＳ３７に進む。ステップＳ３７では、遠隔操作データの内容が「記憶データ転送」コードと一致するか否かを識別し、一致した場合にはステップＳ３８に進み、「記憶データ転送」の保全処理を実行する。ステップＳ３７で不一致の場合は次の処理コードのステップＳ３９に進む。ステップＳ３９では、遠隔操作データの内容が「使用者の識別」コードと一致するか否かを識別し、一致した場合はステップＳ４０に進み、「使用者の識別」の保全処理を実行する。ステップＳ３９で不一致の場合は次の処理コードのステップＳ４１に進む。

【００５８】ステップＳ４１では、遠隔操作データの内容が「電源オフ」コードと一致するか否かを識別し、一致した場合はステップＳ４２に進み、「電源オフ」の保全処理を実行する。ステップＳ４１で不一致の場合は次の処理コードのステップＳ４３に進み、どのコードにも非該当のコードであれば、ステップＳ４５で保全処理システムを終了する。又はステップＳ４４で固定の保全処理として例えば「電源オフ」の保全処理を実行して終了する。

【００５９】上記の説明のように本実施の形態４では、、携帯型電子装置は携帯型電子装置の所有者が予め入力したキーワードを記憶手段に記憶しておき、電波通信手段を媒体にして遠隔操作データを受信し、その識別結果の保全処理コード情報を記録手段に記録し、この記憶手段のキーワードと保全処理コード情報との一致を確認した後で、図６に示す処理を実行することで、携帯型電子装置の保全を実現できるとともに、ケースバイケースで最適の保全処理を選択し、最適の運用を適用することができる効果がある。

【００６０】（実施の形態５）本発明の実施の形態５における保全処理手段の保全処理内容ａについて、図７を参照して説明する。

【００６１】保全処理内容ａは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用しようとしても、携帯型電子装置の本来の機能を停止して他人が使用できなくする「電源オフ」の保全処理である。

【００６２】図７は携帯型電子装置の本来の機能を停止するための「電源オフ」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ４４１において「電源オフ」フラッグがオンかを判定し、「電源オフ」フラッグがオンでない場合はステップＳ４４２に進み、「電源オフ」の保安処理を実行しない。また、「電源オフ」フラッグがオンである場合はステップＳ４４３に移行してパワーオンスイッチ・ディスエーブルフラッグをオンする。そして、ステップＳ４４４で携帯型電子装置の電源を強制的にオフし、「電源オフ」の保全処理を実施し（ステップＳ４４５）、電源オンを禁止する命令が優先的に実行される。

【００６３】このように、遠隔操作データで「電源オフ」保全処理をした場合、マニュアルモードにして携帯型電子装置の電源スイッチをオンしても、制御部はパワーオンシーケンスでフラッグがオンを確認し、電源をオフに移行させる。従って、携帯型電子装置の電源がオンにならないので、例え盗難に遭遇したような場合であっても他人に使用されず、回線使用料金が無謀に請求されることがない。

【００６４】この「電源オフ」保全処理は、携帯型電子装置の電源スイッチをオフにしてしまうもので、手順上極めて明解な保全処理であり、所有者が携帯型電子装置を盗まれたり紛失したことに気が付いた場合において、以下に示す保全処理内容ｂ～ｊなどで処理できなかった折に最終的に施す保全処理として活用するのに適している。更に他の保全処理内容ｂ～ｊなどで処理した後、「電源オフ」の保全処理を複合させて活用するようにしてもよい。

【００６５】また、「電源オフ」保全処理は、携帯型電子装置の本来の機能を停止することを目的にするもので、上記のパワーオンスイッチ・ディスエーブルフラッグをオンする以外の手段で、マイクロコンピュータのリセットオンや駆動用発振機能オフなどの手段などあらゆるハード手段も含むものである。

【００６６】多くの保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００６７】特に、本実施の形態５では、電源が入らな

いので装置の基本機能を殺す保全処理により、装置の紛失者にとって最小限度の損失に抑えることができる。

【００６８】（実施の形態６）本発明の実施の形態６における保全処理手段の保全処理内容ｂについて、図８を参照して説明する。

【００６９】保全処理内容ｂは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、視覚または聴覚によりアラームを発生して使用を禁止する「警告発生」の保全処理である。例えば、置き忘れや紛失された携帯型電子装置の表示部に所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示すること、またはスピーカから呼び掛けを音声を発信することにより、拾得者から所有者への返還を容易にする。

【００７０】図８は携帯型電子装置の本来の機能を停止するための「警告発生」の保全処理ルーチンを示すフローチャートである。「警告発生」の保全処理ルーチンでは、まず、ステップＳ２４１において「警告発生」フラッグがオンかを判定し、「警告発生」フラッグがオンでない場合はステップＳ２４２に進み、「警告発生」の保安処理を実行しない。また、「警告発生」フラッグがオンである場合はステップＳ２４３に移行してスピーカからアラーム音を発生させ、また液晶などの表示部の全面を点滅させる（ステップＳ２４４）。そして、アラーム音の発生時間及び表示部の表示時間をカウントし（ステップＳ２４５）、所定時間経過したかを判定する（ステップＳ２４６）。ここで、所定時間経過しない場合はステップＳ２４３に戻り、所定時間経過した場合はステップＳ２４１に戻る。

【００７１】このように、例え盗難や紛失に遭遇したような場合であっても他人がアラーム音を止めることがでず、表示部の点滅の繰り返し表示を止めることができない。したがって、紛失した場合に第３者に発見し拾得しやすく、拾得者が使用することを防止し所有者に返還させる。

【００７２】ただし、警告音や表示部の点滅の繰り返しは、携帯型電子装置の電池の消費電力が大きいため、第３者に発見されずに電池の消耗になる恐れがあるので、一定時間のみ駆動させる。

【００７３】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００７４】特に、本実施の形態では、装置の拾得者に警告発生により装置の他人使用の禁止を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、併せて所有者に返還させる効果が大きい。

【００７５】（実施の形態７）本発明の実施の形態７における保全処理手段の保全処理内容ｃについて、図９を参照して説明する。

【００７６】保全処理内容ｃは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者が予め記憶手段に蓄積記憶した連絡先やメッセージを呼び掛け表示し、装置を回収する「メッセージ表示」の保全処理である。例えば、盗まれたり紛失した携帯型電子装置の所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示部に表示すること、またはスピーカーから呼び掛けをすることにより、拾得者が使用することを防止したり、所有者に返還させる。

【００７７】図９は携帯型電子装置の本来の機能を停止するための「メッセージ表示」保全処理のルーチンを示すフローチャートである。まず、ステップＳ２６１において「メッセージ表示」フラッグがオンかを判定し、「メッセージ表示」フラッグがオンでない場合はステップＳ２６２に進み、「メッセージ表示」の保安処理を実行しない。また、「メッセージ表示」フラッグがオンである場合はステップＳ２６３に移行してメッセージコード番号によりメッセージ内容を選択し、記憶した所定の表示内容１を表示部に表示する（ステップＳ２６４）。そして、記憶した所定の呼び掛け音１をスピーカから発生させ（ステップＳ２６４Ａ）、メッセージ表示の保全処理を実施する（ステップＳ２６７）。

【００７８】また、メッセージコード番号により別のメッセージ内容を選択した場合は、記憶した所定の表示内容２を表示部に表示する（ステップＳ２６５）。そして、記憶した所定の呼び掛け音２をスピーカから発生させ（ステップＳ２６５Ａ）、メッセージ表示の保全処理を実施する（ステップＳ２６７）。また、メッセージコード番号により更に別のメッセージ内容を選択した場合は、記憶した所定の表示内容３を表示部に表示する（ステップＳ２６６）。そして、記憶した所定の呼び掛け音３をスピーカから発生させ（ステップＳ２６６Ａ）、メッセージ表示の保全処理を実施する（ステップＳ２６７）。

【００７９】このように「メッセージ表示」の保全処理のルーチンでは、メッセージ表示フラッグをオンすると事前に記憶した所定の表示内容が液晶などの表示部に表示できるから、携帯型電子装置を所有者以外の他人が使用すると、所有者が予め入力して記憶手段に蓄積記憶した連絡先やメッセージが表示されることになる。

【００８０】この場合、「メッセージ表示」の保全処理はコード番号により複数の使い分けが可能である。例えばコード番号により「所有者連絡先」、「住所」、「電話番号」、「拾得者へお願い」、「拾得者へのお礼内容」など、所有者が盗難や紛失された場所や場合によってメッセージを使い分けができる。例えば「拾得者へお願い」の場合は『この装置を拾って頂いた方は、お手数ですが次にご連絡頂きますようにお願い致します。私は○○です。電話番号が○○です。よろしくお願い致します。』のメッセージ内容を表示しスピーカから呼び掛け

をする。また「拾得者へのお礼内容」の場合は『この装置を拾った方は、お手数ですが次にご連絡して下さい。謝礼に○○を差し上げます。電話番号が○○です。返却住所が○○です。』のメッセージ内容を表示しスピーカから呼び掛けをする。

【００８１】このように本実施の形態では、盗難や紛失された携帯型電子装置の所有者の住所と電話番号などの連絡先および拾得者へのメッセージなどを表示部に表示すること、またはスピーカから呼び掛けをすることにより、拾得者が所有者に連絡をすることができれば、所有者に返還させることができる。また、拾得者が使用するたびに返却要求のメッセージで訴えると、拾得者が使用することを回避させることができる。

【００８２】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００８３】特に、本本実施の形態では、装置の拾得者にメッセージ表示により装置の返却を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、所有者に返還できる効果がある。

【００８４】（実施の形態８）本発明の実施の形態８における保全処理手段の保全処理内容ｄについて、図１０を参照して説明する。

【００８５】保全処理内容ｄは、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、本来の機能を停止し、所有者が予め入力して記憶手段に蓄積記憶した連絡先にのみ交信する「所有者連絡発信」の保全処理である。例えば、盗難や紛失された携帯型電子装置の所有者が予め契約した警備会社の連絡先を登録しておけば、拾得者が無断使用しようとしてダイヤルした場合にも、警備会社の連絡先にすべて交信する。

【００８６】図１０は携帯型電子装置の本来の機能を停止するための「所有者連絡発信」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ３０１において「所有者連絡発信」フラッグがオンかを判定し、「所有者連絡発信」フラッグがオンでない場合はステップＳ３０２に進み、「所有者連絡発信」の保安処理を実行しない。また、「所有者連絡発信」フラッグがオンである場合はステップＳ３０３に移行して、予め設定した連絡先の内容を記憶手段から選択し、記憶した所定の連絡先１を表示部に表示する（ステップＳ３０４）。そして、記憶した所定の連絡先１に自動発信・接続し（ステップＳ３０４Ａ）、所有者連絡発信の保全処理を実施する（ステップＳ３０７）。

【００８７】また、別の連絡先内容を選択した場合は、記憶した所定の連絡先２を表示部に表示する（ステップＳ３０５）。そして、記憶した所定の連絡先２に自動発信・接続し（ステップＳ３０５Ａ）、所有者連絡発信の保全処理を実施する（ステップＳ３０７）。

【００８８】このように「所有者連絡発信」の保全処理のルーチンでは、所有者連絡発信フラッグをオンすると事前に記憶した所定の連絡先にのみ交信可能になる。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、所有者連絡発信フラッグのオンを確認し、所定の連絡先に優先的に交信が移行する。したがって、所有者が予め所有者自身を連絡先に登録した場合は、所有者は拾得者と必ず交信ができ、拾得者に直に返却の依頼ができる。また、この場合、拾得者は所有者以外への交信使用することができないから、盗難にあった場合でも第３者は使用することができず、回線使用料金が無謀に請求されることがない。

【００８９】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００９０】特に、本実施の形態では、装置の拾得者の使用に対し所有者連絡発信により連絡が取れ装置の返却を訴える保全処理により、装置の紛失者にとって他人に使用されることを防止し、所有者に返還できる効果がある。

【００９１】（実施の形態９）本発明の実施の形態９における保全処理手段の保全処理内容ｅについて、図１１を参照して説明する。

【００９２】保全処理内容ｅは、盗難や紛失された携帯型電子装置の本来の機能のうちを所有者があらかじめ入力した機能を停止する「発信機能禁止」の保全処理である。装置の本来の機能のうち例えば、ダイヤル入力機能を停止することにより発信通話を禁止したり、記録機能のみを停止することにより所有者に関する個人情報だけをセキュリティ保護するなど部分的な機能のみを保全処理する。

【００９３】図１１は携帯型電子装置の本来の機能を停止するための「発信機能禁止」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ２８１において「発信機能禁止」フラッグがオンかを判定し、「発信機能禁止」フラッグがオンでない場合はステップＳ２８２に進み、「発信機能禁止」の保安処理を実行しない。また、「発信機能禁止」フラッグがオンである場合はステップＳ２８３に移行して、発信要求コード番号を無効にする発信機能をオフし、発信機能禁止の保全処理を実施する（ステップＳ２８４）。

【００９４】このように「発信機能禁止」の保全処理ルーチンでは、発信機能禁止フラッグをオンすると発信通話を禁止する。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、発信機能禁止フラッグがオンを確認し、発信通話の禁止へ優先的に移行する。したがって、拾得者は発信通話ができず他人への

交信使用することができず、盗難に遭遇した場合でも第３者に使用されることがなく、回線使用料金が所有者に無謀に請求されることがない。

【００９５】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【００９６】特に、本実施の形態では、装置の拾得者の使用に対し発信機能禁止の保全処理により、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【００９７】（実施の形態１０）本発明の実施の形態１０における保全処理手段の保全処理内容ｆについて、図１２を参照して説明する。

【００９８】保全処理内容ｆは、盗難や紛失された携帯型電子装置の記録手段からデータの出力を禁止する「データ出力禁止」の保全処理である。例えば、携帯型電子装置の所有者に関する個人情報や内部機密データを特定な記憶指定ロックで保管し、予め指定したキーワード以外の手順では開示できないようにする。

【００９９】図１２は携帯型電子装置の本来の機能を停止するための「データ出力禁止」保全処理のルーチンを示すフローチャートである。まず、ステップＳ３４１において「データ出力禁止」フラッグがオンかを判定し、「データ出力禁止」フラッグがオンでない場合はステップＳ３４２に進み、「データ出力禁止」の保安処理を実行しない。また、「データ出力禁止」フラッグがオンである場合はステップＳ３４３に移行して、発信要求コード番号を無効にする発信機能のオフ内容を選択し、データ出力禁止の保全処理を実施する（ステップＳ３４４）。

【０１００】このように「データ出力禁止」の保全処理ルーチンでは、データ出力禁止フラッグをオンするとデータ出力を禁止する。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、データ出力禁止フラッグがオンを確認し、データ出力を禁止する処理に優先的に移行する。したがって、拾得者や第３者はデータを出力できず、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。また、盗難や紛失された後「データ出力禁止」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎなく、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。

【０１０１】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【０１０２】特に、本実施の形態では、装置の内部の個人データや情報を保護するデータ出力禁止の保全処理により、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【０１０３】（実施の形態１１）本発明の実施の形態１１における保全処理手段の保全処理内容ｇについて、図１３を参照して説明する。

【０１０４】保全処理内容ｇは、盗難や紛失された携帯型電子装置の記録手段のデータを消却し、他人に見られたり使用されないようにする「記憶データ消去」の保全処理であり、携帯型電子装置の記録部の所有者に関する個人情報やデータを消去し、他人の開示を回避する。

【０１０５】図１３は携帯型電子装置の本来の機能を停止するための「記憶データ消去」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ３２１において「記憶データ消去」フラッグがオンかを判定し、「記憶データ消去」フラッグがオンでない場合はステップＳ３２２に進み、「記憶データ消去」の保安処理を実行しない。また、「記憶データ消去」フラッグがオンである場合はステップＳ３２３に移行して、記憶手段の所定のエリアのデータを消去し、記憶手段のユーザーエリアのデータ（個人情報、装置の固有情報、通話番号等）の選択を禁止する。その後、記憶データ消去の保全処理を実施する（ステップＳ３２４）。

【０１０６】このように「記憶データ消去」の保全処理ルーチンでは、記憶データ消去フラッグをオンすると記憶データが消去される。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、記憶データ消去フラッグがオンを確認し、記憶データを消去する処理に優先的に移行する。したがって、拾得者や第３者が盗難や紛失された携帯型電子装置を使用としても記憶データ消去されており、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。また、盗難や紛失された後「記憶データ消去」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎず、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。

【０１０７】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されての所有者の害を被ることを排除する所定のセキュリティを高める効果がある。

【０１０８】特に、本実施の形態では、装置の内部の個人データや情報を保護する記憶データ消去の保全処理で、装置の紛失者にとって他人に使用されることを防止し不当な使用に伴う料金が生じることを回避し、個人データや情報を他人に悪用されることを阻止できる効果がある。

【０１０９】（実施の形態１２）本発明の実施の形態１２における保全処理手段の保全処理内容ｈについて、図１４を参照して説明する。

【０１１０】保全処理内容ｈは、盗難や紛失された携帯型電子装置の通信回線番号を消滅し、他人が使用できなくする「通信回線番号消滅」の保全処理であり、他人に悪用され通話料金の請求を回避する。

【０１１１】図１４は携帯型電子装置の本来の機能を停止するための「通信回線番号消滅」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ３６１において「通信回線番号消滅」フラッグがオンかを判定し、「通信回線番号消滅」フラッグがオンでない場合はステップＳ３６２に進み、「通信回線番号消滅」の保安処理を実行しない。また、「通信回線番号消滅」フラッグがオンである場合はステップＳ３６３に移行して、通信ダイヤルスイッチディスエーブルフラッグをオンする。そして、ステップＳ３６４で携帯型電子装置の電源を強制的にオフし、通信回線番号消滅の保全処理を実施する（ステップＳ３６５）。

【０１１２】このような「通信回線番号消滅」の保全処理ルーチンでは、通信回線番号消滅フラッグをオンすると記憶された携帯型電子装置の通信回線番号を消滅される。すなわち、盗難や紛失された携帯型電子装置を所有者以外の他人が使用すると、通信回線番号消滅フラッグがオンを確認し、携帯型電子装置に記憶された通信回線番号を消去する処理に優先的に移行する。したがって、拾得者や第３者が盗難や紛失された携帯型電子装置を使用としても記憶されていなければならない通信回線番号が消滅され、他人が全く利用することができない。また、盗難や紛失された後「通信回線番号消滅」の保全処理された携帯型電子装置は所有者以外の他人にとっては全くの単なる無機物にすぎなく、所有者の損失は携帯型電子装置のハードだけで、所有者の財産または情報に関わるセキュリティを高めることができる。また、通信回線番号は、携帯型電子装置の製造者または販売者のみが特殊な方法で入力することができ、電源をオフしても登録内容が保持される内部記憶媒体部に１度だけ記憶された各装置の固有の番号である。

【０１１３】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まらたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることによる所有者が害を被ることを排除する所定のセキュリティを高める効果がある。

【０１１４】特に、本実施の形態では、装置の拾得者の使用に対し通信回線番号を消滅させて発信機能を不可能にする保全処理であるから、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる　果がある。

【０１１５】（実施の形態１３）本発明の実施の形態１３における保全処理手段の保全処理内容ｉについて、図１５を参照して説明する。

【０１１６】保全処理内容ｉは、盗難や紛失された携帯型電子装置の記録手段のデータを他の所定の電子装置に転送し、記憶データを回収する「記憶データ転送」の保全処理であり、携帯型電子装置の記録部の所有者に関する個人情報やデータを他の所定の電子装置に転送し、その後、該装置の記録部の個人情報やデータを他の所定の電子装置が流用する。

【０１１７】図１５は携帯型電子装置の本来の機能を停止するための「記憶データ転送」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ３８１において「記憶データ転送」フラッグがオンかを判定し、「記憶データ転送」フラッグがオンでない場合はステップＳ３８２に進み、「記憶データ転送」の保安処理を実行しない。また、「記憶データ転送」フラッグがオンである場合はステップＳ３８３に移行して記憶手段から記憶データを読み出し、記憶データを送信する（ステップＳ３８４）。その後、データ転送が完了したかを判定する（ステップＳ３８５）。ここで、データ転送が完了しない場合はステップＳ３８３に戻り、データ転送が完了した場合はステップＳ３８６に移行して記憶部を破壊しデータを消去する。そして、記憶データ転送の保全処置を実施する（ステップＳ３８７）。

【０１１８】このように「記憶データ転送」の保全処理ルーチンでは、記憶データ転送フラッグをオンすると記憶データを転送し回収される。これにより、盗難や紛失された携帯型電子装置に記憶させた個人情報やデータを読み取り転送させることができ、更にその後装置の記録手段の記憶データを消去する処理に優先的に移行する。したがって、携帯型電子装置を盗難や紛失された時に本保全処理により、所有者は他の所定の電子装置に記憶データを読み取り転送し回収でき、その後で元の記憶データを消去できるため、拾得者や第３者が盗難や紛失された携帯型電子装置を使用としても記憶データは消去されており、所有者のデータや個人情報を所有者以外の他人が覗いたり利用することができない。

【０１１９】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置が盗まれたり紛失しても、携帯型電子装置の個人データの保護や他人に使用されることによる所有者が害を被ることを排除する所定のセキュリティを高める効果がある。

【０１２０】特に、本実施の形態では、装置の内部の個人データや情報を遠隔操作で転送する「記憶データ転送」の保全処理により、装置の紛失者にとって他人に使用される前に内部の個人データや情報を転送回収して、その後装置内部の記憶データを消去し、装置の紛失者にとって他人に使用されることを防止し、不当な使用に伴う料金が生じることを回避できる効果がある。

【０１２１】（実施の形態１４）本発明の実施の形態１４における保全処理手段の保全処理内容ｊについて、図１６を参照して説明する。

【０１２２】保全処理内容ｉは、使用者を識別し、所有者以外の他人が携帯型電子装置を使用を不可能にする「使用者の識別」の保全処理である。使用者の識別は、例えばパスワード入力、指紋認識、声紋認識など使用者の識別手段により、所有者以外の人が携帯型電子装置を使用した時に保全処理が実行される。

【０１２３】図１６は携帯型電子装置の本来の機能を停止するための「使用者の識別」の保全処理ルーチンを示すフローチャートである。まず、ステップＳ４０１において「使用者の識別」フラッグがオンかを判定し、「使用者の識別」フラッグがオンでない場合はステップＳ４０２に進み、「使用者の識別」の保安処理を実行しない。また、「使用者の識別」フラッグがオンである場合はステップＳ４０３に移行して装置の発信通話機能を先ずオフし、次いで使用者識別番号かを判定する（ステップＳ４０４）。ここで、使用者識別番号でない場合はステップＳ４０２に戻り、使用者識別番号の場合はステップＳ４０５、ステップＳ４０６、ステップＳ４０７のいずれかへ移行して使用者の識別を行う。

【０１２４】使用者の識別の一つは、使用時にパスワードの入力を要求し、この入力パスワードと携帯型電子装置の所有者が予め設定し登録したパスワードと比較し（ステップＳ４０５）、パスワードが一致したかを判定する（ステップＳ４０５Ａ）。ここで、一致した場合はステップＳ４０９に移行して正常使用を可能にする。また、不一致の場合は、パスワードの誤入力に対するリトライ回数を３回に定め（ステップＳ４０５Ｂ）、パスワードの誤入力が３回以上あった場合は更に強度の保全処理を実行する（ステップＳ４０８）。この時の所有者が予め設定するパスワードは、電源をオフしても登録内容が保持される記憶部に１度だけ記憶する。使用前にパスワードの入力してから運用する保全処理は従来もあったが、通常時には厄介なこともあり平常はその保全処理を解除していることが多い。しかし本保全処理は、携帯型電子装置の所有者が、その携帯型電子装置が盗まれたり紛失した場合に、保全を要する携帯型電子装置に遠隔操作データを送信し、パスワードによる保全処理の機能を働かさせるところに特徴を有する。

【０１２５】また、使用者の識別の他の例としては、携帯型電子装置を使用する者に指紋の入力を要求し、この指紋と携帯型電子装置の所有者が予め設定し登録した指紋とを比較し（ステップＳ４０６）、指紋が一致したかを識別する（ステップＳ４０６Ａ）。ここで、使用者の指紋入力する場合は、例えば携帯電話機を持つ手の親指が当たる部分に指紋を検出する機能と指紋を認識する機能を付加することで可能になる。したがって、指紋の一致が認識された場合はステップＳ４０９に移行して正常使用を可能にする。また、指紋の不一致が認識された場合は、指紋の誤入力に対するリトライ回数を３回に定め（ステップＳ４０６Ｂ）、指紋の誤入力が３回以上あった場合は更に強度の保全処理を実行する（ステップＳ４０８）。

【０１２６】また、使用者の識別の更に他の例としては、パスワードを音声化し、予め登録したパスワードの音声データ（声紋）とマイクから入力した声紋を照合し（ステップＳ４０７）、声紋が一致したかを認識する（ステップＳ４０７Ａ）。ここで声紋の一致が認識された場合はステップＳ４０９に移行して正常使用を可能にする。また、声紋の不一致が認識された場合は、声紋の誤入力に対するリトライ回数を３回に定め（ステップＳ４０７Ｂ）、声紋の誤入力が３回以上あった場合は更に強度の保全処理を実行する（ステップＳ４０８）。

【０１２７】このように「使用者の識別」の保全処理ルーチンでは、使用者の識別フラッグをオンすると使用者の識別手段によりパスワード、指紋、声紋を識別し、所有者以外の人が携帯型電子装置を使用を検出した場合には使用者の識別フラッグがオンを確認し、装置の発信通話を禁止する処理に優先的に移行する。したがって、拾得者は発信通話ができず他人への交信使用することができない。

【０１２８】他の保全処理のうち１つ以上の処理を遠隔操作データで実施する結果により、例え携帯型電子装置を盗難や紛失されても、携帯型電子装置の個人データの保護や他人に使用されることを排除する所定のセキュリティを高める効果がある。

【０１２９】（実施の形態１５）次に、本発明の請求項１５に対応する実施の形態１５の保全処理について説明する。この実施の形態による保全処理内容は、次に示す内容から構成される。

【０１３０】保全処理内容ａは、携帯型電子装置に送信した相手に、所有者が受信できない事情にある所定の情報を相手に送信する保全処理であり、送信した相手に、個人情報やデータを所有者が受信できない事情にある旨を知らせ、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されることを保全する。

【０１３１】保全処理内容ｂは、携帯型電子装置に送信した相手からの受信情報を受信する機能を停止する保全処理であり、他人の拾得者に個人情報やデータが漏洩されないように、相手からの受信情報を受信する機能を停止し保全する。

【０１３２】保全処理内容内容ｃは、携帯型電子装置に送信した相手に、話中または使用中のデータを送信する保全処理であり、送信した相手が、個人情報やデータを所有者に送信する前に話中または使用中の信号データを一方的に送信して、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されるこ

とを保全する。

【０１３３】保全処理内容ｄは、携帯型電子装置に送信した相手に、送信情報を送信する機能を停止する保全処理であり、送信した相手が、個人情報やデータを所有者に送信する前に通信手続きの動作において、例えばアクセス信号を送信せずに、送信情報を送信する機能を停止し、交信を回避する。

【０１３４】保全処理内容ｅは、携帯型電子装置に送信した相手に、所有者が予め入力して記憶手段に蓄積記憶した紛失メッセイジを送信する保全処理であり、保全処理内容ｃにおける話中または使用中の信号データの代わりに、予め入力して記憶手段に蓄積記憶した紛失メッセージを一方的に送信して、送信することを未然に回避させることで、他人の拾得者に個人情報やデータが漏洩されることを保全する。

【０１３５】保全処理内容ｆは、携帯型電子装置に送信した相手に、該携帯型電子装置の使用を防止する保全処理であり、他人の拾得者が拾得した携帯型電子装置を使用した個人情報やデータを、所有者の個人情報やデータとして相手が交信したことによる問題を回避するために、転送先を固定し記憶された住所など消去するもので、他人の開示を回避する。

【０１３６】以上の保全処理のうち１つ以上の処理を実施する結果により、例え携帯型電子装置を盗まれたり紛失しても、その装置の所有者に送信した相手にとって、携帯型電子装置の個人データの保護や他人に使用されて所有者が害を被ることが排除され、所定のセキュリティを高めることができる。

【０１３７】（実施の形態１６）次に、本発明の請求項１６に対応する実施の形態１６の保全処理について説明する。この実施の形態は、電波通信手段を伝送媒体とし、所有者が予め入力して記憶手段に蓄積記憶したキーワード信号を受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の保全機能を駆動し、所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたところにある。

【０１３８】図１において、携帯型電子装置１を盗まれたり紛失した所有者は、一般公衆電話や携帯電話としてのＰＨＳなど電話機３を操作して携帯型電子装置１に電話をかける。この場合市内や市外の一般公衆電話３Ａから公衆回線網２ｃを介して、またＰＨＳデータ通信装置や携帯電話としてのＰＨＳ３から無線通信回線２ｂを介して保全を要する携帯型電子装置１に遠隔操作データを送信する。

【０１３９】次に、本実施形態の保全処理動作について図１７に示す保全確認のルーチンを用いて説明する。

【０１４０】盗難や紛失した携帯型電子装置１は、多くの場合に他人が拾得していることがあり、通話が可能である。次に携帯型電子装置１を盗まられたり紛失した所有者は、所有者が予め入力して記憶手段に蓄積記憶したキーワード信号を送信する。記憶手段に蓄積記憶したキーワード信号を受信した場合に、該携帯型電子装置１は遠隔操作データを受信する受信部１１で受信し（ステップＳ１７１）、受信した遠隔操作データが予め記憶された所定のキーワード信号と一致することを識別する識別部１２で判定する（ステップＳ１７２）。識別部１２の識別結果により一致が確認された場合のみ保全確認信号を発信する（ステップＳ１７３）。この保全確認信号の指示により他の機能を強制的にオフし（ステップＳ１７４）、次いで保全部１３が強制的に携帯型電子装置の保全機能を駆動し（ステップＳ１７５）、携帯型電子装置の所有者が害を被ることを排除する所定の保全処理をするように動作する。

【０１４１】特に、本実施の形態では、装置の紛失者が予め入力して記憶手段に蓄積記憶したキーワード信号を送信し、強制的に携帯型電子装置の保全機能を駆動し、装置の紛失者にとって他人に使用されることを防止できる。

【０１４２】（実施の形態１７）次に、請求項１７に対応する実施の形態１７について、図１８を参照して説明する。この実施の形態では、所有者が予め入力して記憶手段に蓄積記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により、強制的に携帯型電子装置の接続を行い、所有者が害を被ることを排除する所定のセキュリティを高める保全処理手段を設けたものである。

【０１４３】すなわち、第１回目の受信の呼び出し信号回数をカウントし（ステップＳ１０１）、そのカウント値が予め設定した第１回目のコール回数と識別したかを判定する（ステップＳ１８２）。ここで、否定判定された場合はステップＳ１８１に戻り、肯定判定された場合はステップＳ１８３に進む。ステップＳ１８３では、第２回目の受信の呼び出し信号回数をカウントし、そのカウント値が予め設定した第２回目のコール回数と識別したかを判定する（ステップＳ１８４）。ここで、否定判定された場合はステップＳ１８１に戻り、肯定判定された場合はステップＳ１８５に進む。

【０１４４】ステップＳ１８５では、第３回目の受信の呼び出し信号回数をカウントし、そのカウント値が予め設定した第３回目のコール回数と識別したかを判定する（ステップＳ１８６）。ここで、否定判定された場合はステップＳ１８１に戻り、肯定判定された場合はステップＳ１８７に進む。ステップＳ１８７では保全システムを立ち上げ、次の受信の呼び出し信号回数から保全内容を識別したかを判定する（ステップＳ１８８）。保全内容を識別した場合はステップＳ１８９に進み、遠隔操作データの保全内容を解析する。そして、遠隔操作データの識別結果に応じた保全処理を実施する（ステップＳ１９０）。

【０１４５】このように盗難や紛失した携帯型電子装置

を拾得した者が応答したとか、交信ができない事態の場合においても、予め入力して記憶手段に蓄積記憶した呼び出し信号回数のパターンを受信した場合に、遠隔操作データの識別結果により強制に電源供給を中断し、即停止するなどの所定の保全処理内容を適用するように動作する。

【０１４６】上記の呼び出し信号回数のパターンは、例えば第１回目の１０回呼び出し後一旦フック回線をオフし、第２回目の５回呼び出し後一旦フック回線をオフし、第３回目の８回呼び出し後一旦フック回線をオフするものであり、この呼び出し信号回数のパターンを所定時間の期間に繰り返すパターンを受信した場合に、所定の保全処理内容を適用する。

【０１４７】なお、本発明の請求項８は、実施の形態４における携帯型電子装置の遠隔操作データの処理ルーチンで、図６のステップＳ２０、ステップＳ２１によるキーワード識別に相当する遠隔操作か否かを識別する方法を代替えするものである。その結果により個々の保全処理の内容については、上記と同様のため説明を省略する。

【０１４８】本実施の形態による保全処理は、携帯型電子装置を情報携帯端末電話装置に適用した実例であるが、一般的な情報携帯端末機やＰＨＳやコードレス電話機においても適用できるものである。

【０１４９】特に、本実施の形態では、装置の拾得者が応答しなとか、交信ができない事態の場合においても、呼び出し信号回数のパターンによる遠隔保全処理を起動させ、装置の紛失者にとって他人に使用されることを防止できる。

【０１５０】（実施の形態１８）次に、本発明の請求項１８に相当する実施の形態１８の携帯型電子装置保全システムについて図１９を参照しながら説明する。

【０１５１】この実施の形態では、携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置保全システムである。特に微弱電波或いは超音波などを用いた子機を備えた携帯型電子装置に関するもので、実施の形態１のように、この種の携帯型電子装置はいつか如何なる時でも遺失の件数は膨大し、小型携帯上は優れており便利であるが盗難に合いやすい。これらの遺失対策はそれらの所有者が細心の注意を払う以外にないが、それが如何に効果の少ない方法であるかを多く体験していることである。

【０１５２】この問題を解決する手段として本実施の形態では、微弱電波或いは超音波或いは誘導電波などを発振する発振手段と、それを本体に送信する微弱電力送信手段を有する子機を備え、該子機からの保全処理を促すための発振データを受信する手段、受信した操作データを識別する手段、該識別の結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を備えてた携帯型電子装置（本体）で構成し、上記微弱電力送信手段を有する子機は、鎖付きのペンダントやピアスのように身近に携帯する小型軽量が望まれる。子機は、服装のポケットなどにしっかりと挿入できるようにフックやベルト付きにし、またはピアスやペンダントに内蔵し子機自身の紛失を防ぐものである。

【０１５３】本体の携帯型電子装置は子機からの保全処理を促すための発振データを受信する受信手段を有し、該受信した操作データを識別する手段で、所定の保全手段を動作するものである。また前記微弱電力送信手段の送信する信号が該受信手段に着信する距離を例えば数メートル程となるように設定し、その通信可能距離以上に上記送受信手段、すなわち本体と子機との両者が離れると着信信号レベルが所定以下になり、該受信した操作データを識別する手段は、本体の携帯型電子装置が所定の距離以上に所有者から離れた、即ち所有者が本体の携帯型電子装置を置き忘れたか遺失したものと識別する。そして該識別の結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段を動作させる。保全手段は、例えば所有者にその旨を気付かせるように警告する警告ブザーを鳴らすことや、携帯型電子装置本体に保全処理を促すための前記実施の形態１のように各種の保全機能を起動させる。

【０１５４】図１９は、本実施の形態１８の一例を示す構成図である。同図でにおいて、子機における発振器２１からの出力信号を伝送部２２で変調増幅し、微弱電力送信手段２３からアンテナを通して所定の微弱電力信号を送信する。

【０１５５】一方、該信号を本体のアンテナから微弱電力受信部２４で受信する。受信信号は伝送部２５で復調増幅され、検波部２６により検波した後、その受信レベルが予め設定したレベル以下かどうかを判定部２７で判別し、受信のレベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する。子機と本体との空間間距離が所定の距離に比べて離れると本体に保全処理を促すための各種の保全処理を行う保全手段２８が動作し、例えば所有者にその旨を気付かせるように警告ブザーを鳴らす。

【０１５６】上記のように、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に、本システムが作動して未然に紛失または置き忘れを防止し回避することができる。また所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【０１５７】（実施の形態１９）図２０は、本発明の請求項１９に対応する実施の形態１９の構成を示す機能ブロック図である。同図において、子機は発振器４１、発振器４１からの出力信号を変調増幅する伝送部４２、伝送部４２からの信号を本体へ送信するとともに本体から

の信号を受信する微弱電力伝送手段４３、微弱電力伝送手段４３の受信信号を復調増幅する伝送部４４、復調信号を検波する検波部４５、検波信号の受信レベルが予め設定したレベル以下かどうかを判別し、かつ受信レベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する判定部４６、子機保全のための各種の保全処理を行う保全手段４７、信号の交信をリセットするリセット部４８から構成されている。

【０１５８】また、本体は子機からの信号を受信するとともに子機へ進行を送信する微弱電力伝送手段４９、微弱電力伝送手段４９の受信信号を復調増幅する伝送部５０、復調信号を検波する検波部５１、検波信号の受信レベルが予め設定したレベル以下かどうかを判別し、かつ受信レベルによって子機と本体との空間距離が所定の距離以上かどうかを判別する判定部５２、本体保全のための各種の保全処理を行う保全手段５３、信号の交信をリセットするリセット部５４、発振器５５、発振器５５からの出力信号を変調増幅して微弱電力伝送手段４９へ出力する伝送部５６から構成されている。

【０１５９】この構成において、図１９に示し場合と同様に形態型電子装置の本体と子機間の距離が、例えば数メートル程度離れることで通信可能距離以上になると着信信号レベルが所定以下になり、該受信した操作データを識別する判定部４６及び５２は、本体の携帯型電子装置が所定の距離以上に所有者から離れた、即ち所有者が本体の携帯型電子装置を盗難および置き忘れたか遺失したものと識別すると、その識別結果により携帯型電子装置の所有者が害を被ることを排除する所定の保全手段４７及び５３が動作を開始し、未然に盗難および紛失または置き忘れを防止し回避することができる。保全手段４７及び５３は、例えば所有者にその旨を気付かせるように警告する本体及び子機の一方または双方で警告ブザーを鳴らすことや、携帯型電子装置本体に保全処理を促すための前記実施の形態のように各種の保全機能を起動させる。

【０１６０】このように本体及び子機に警告を発生する手段を有することによって、所有者が携帯型電子装置を盗難および紛失または置き忘れそうになった場合に、本システムの保全手段が作動して未然に盗難および紛失または置き忘れを防止し回避することができる。特に盗難および置き引きに遭遇した場合に、警告音を発生することの効果や危険性を考慮し、子機から警告音を発生させずバイブレータ振動で所有者に報知することで周囲の人々に気付かれないで紛失または置き忘れを回避できる。また、警告音を発生させて周囲の人々に気付かせたいのか、または周囲の人々に気付かれないで解決するか切り替えることができる。

【０１６１】更に、子機に着信信号レベルを換算し本体と子機との両者間の距離を表示する機能を設ける携帯型電子装置においては、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に、本体と子機との両者間の距離を表示する子機により、本体の存在する位置を検索することができる。例えば部屋内で本体を見失った場合に、子機と本体間の距離の表示の変化で本体が存在する位置を見つけ出すことが可能になる。

【０１６２】また、上記の本実施の形態において、信号の交信をリセットするリセット部を付加することが運用上便利である。リセット部を付加することは、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に動作した後、再度本実施例の機能を運用させる上で極めて大きい効果を有する。

【０１６３】上記の説明により本発明のように携帯型電子装置を紛失または置き忘れを防止するための携帯型電子装置の保全システムを容易に実施することができ、携帯型電子装置を紛失または置き忘れを防止する上で大きな効果を有する。

【０１６４】なお、上記実施の形態における保全処理は携帯型電子装置を情報携帯端末電話装置に適用した場合について説明したが、一般的な情報携帯端末機やＰＨＳやコードレス電話機においても適用できるものである。

【０１６５】

【発明の効果】以上のように本発明の携帯型電子装置の保全システムによれば、上記実施例より明らかなように、以下の効果を得ることができる。

【０１６６】携帯型電子装置（ＰＨＳ、携帯電話機も含む電波通信手段を有するデータ処理端末装置）の盗難や紛失に対して、その所有者が遠隔操作するとこにより、携帯型電子装置の所有者が害を被ることを排除する所定の保全手段が動作し、携帯型電子装置の所有者の財産または情報に関わるセキュリティを高めることができる。すなわち、簡単に携帯型電子装置の内部のデータを保護することができ、更に他人に使用されても料金を支払うという不具合を回避することができる。

【０１６７】また、所有者が携帯型電子装置の盗難や紛失に気が付いた場合に、所有者が積極的に保全を要求することにより、携帯型電子装置の所有者に不利益となる要因を防止することができる。即ち、携帯型電子装置の記憶内部および仕様に関してプロテクトをかけて保護することができる。

【０１６８】また、盗難や紛失した携帯型電子装置の所有者に送信した相手にとっても、不適切な状況であることを知らずに携帯型電子装置の所有者と思ってに送信したことで、送信相手または相手情報が害を被る問題が発生するという不具合を回避することができる。即ち、盗難や紛失した携帯型電子装置の所有者や送信相手者が害を被ることを排除することができる。

【０１６９】また、本発明の携帯型電子装置の保全システムによれば、所有者が携帯型電子装置を紛失または置き忘れそうになった場合に、本システムが作動して未然に紛失または置き忘れを防止し回避することができるほ

か、所有者が携帯型電子装置を紛失または置き忘れてしまった場合でも、自動的に本体に保全処理を促すための各種の保全機能を起動させるため、他人に拾得されても装置の所有者の財産または情報に関わるセキュリティを高めることが簡単に実施できる。

【図面の簡単な説明】

【図１】本発明の実施の形態１における携帯型電子装置の保全システムの概略構成図

【図２】本発明の実施の形態２における携帯型電子装置の保全システムの構成を示す機能ブロック図

【図３】本発明の実施の形態２におけるプロトコールのハードウェア構成図

【図４】本発明における携帯型電子装置のネットワークシステムを示す図

【図５】本発明におけるセキュリティを高める保全処理の制御ルーチン図

【図６】本発明における遠隔操作データの処理ルーチン図

【図７】本発明における電源オフの保全処理ルーチンを示すフローチャート

【図８】本発明における警告発生の保全処理ルーチンを示すフローチャート

【図９】本発明におけるメッセイジ表示の保全処理ルーチンを示すフローチャート

【図１０】本発明における所有者連絡発信の保全処理ルーチンを示すフローチャート

【図１１】本発明における発信機能禁止の保全処理ルーチンを示すフローチャート

【図１２】本発明におけるデータ出力禁止の保全処理ルーチンを示すフローチャート

【図１３】本発明におけるデータ出力消去の保全処理ルーチンを示すフローチャート

【図１４】本発明における通信回線番号消滅の保全処理ルーチンを示すフローチャート

【図１５】本発明における記憶データ転送の保全処理ルーチンを示すフローチャート

【図１６】本発明における使用者の識別の保全処理ルーチンを示すフローチャート

【図１７】本発明における保全確認のルーチンを示すフローチャート

【図１８】本発明における呼び出し信号による遠隔操作の処理のルーチンを示すフローチャート

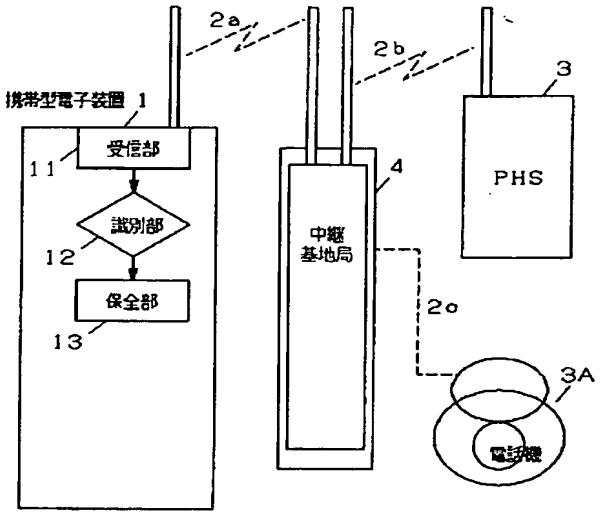
【図１９】本発明の実施の形態１８による携帯型電子装置の保全システムを示す構成図

【図２０】本発明の実施の形態１９による携帯型電子装置の保全システムを示す構成図

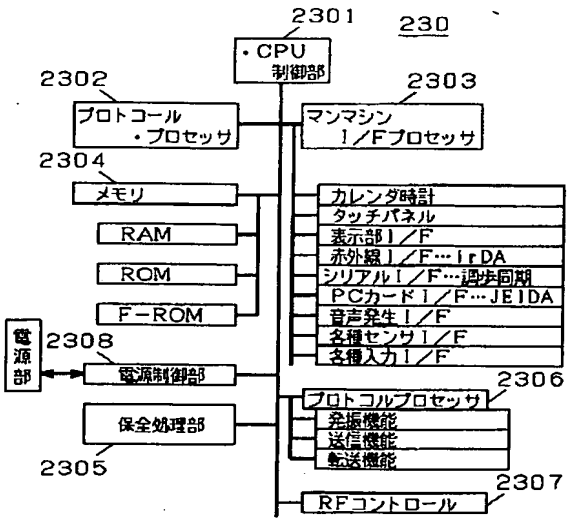
【符号の説明】

１　携帯型電子装置
２ａ，２ｂ，２ｃ　電波通信手段
３　電話機（ＰＨＳ）
３Ａ　電話機
４　中継基地局
１１　受信部（受信手段）
１２　識別部（識別手段）
１３　保全部（保全手段）
２１　発振器
２２　伝送部
２３　微弱電力送信部
２４　微弱電力受信部
２５　伝送部
２６　検波部
２７　判別部
２８　保全手段
３０　公衆ならびに専用回線網
３１　一般の電話機
３２　変復調器付きパソコン
３３　基地局
３４　基地局
３５　基地局
３６　網管理局
４１　発振器
４２　伝送部
４３　微弱電力伝送手段
４４　伝送部
４５　検波部
４６　判別部
４７　保全手段
４８　リセット部
４９　微弱電力受信部
５０　伝送部
５１　検波部
５２　判別部
５３　保全手段
５４　リセット部
５５　発振器
５６　伝送部

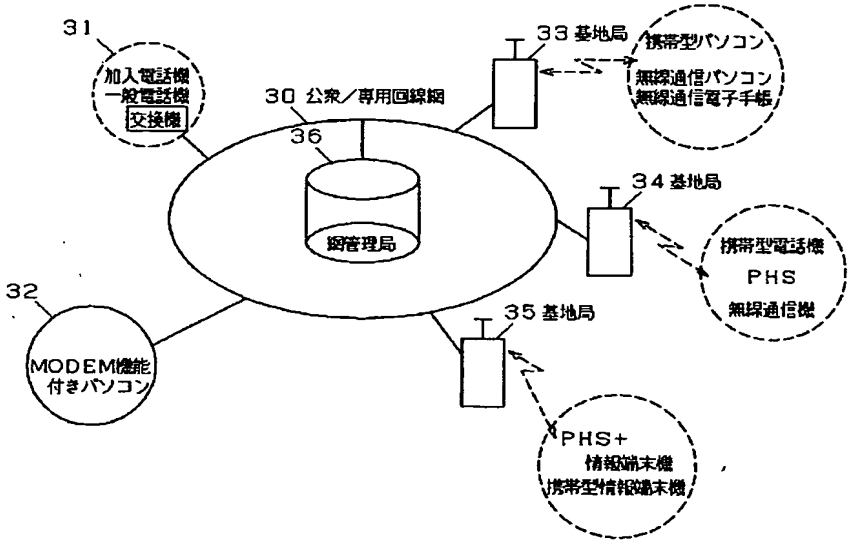
【図１】



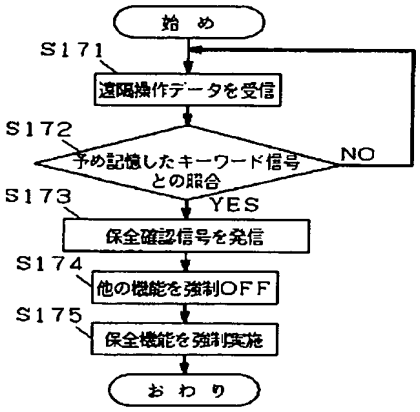
【図３】



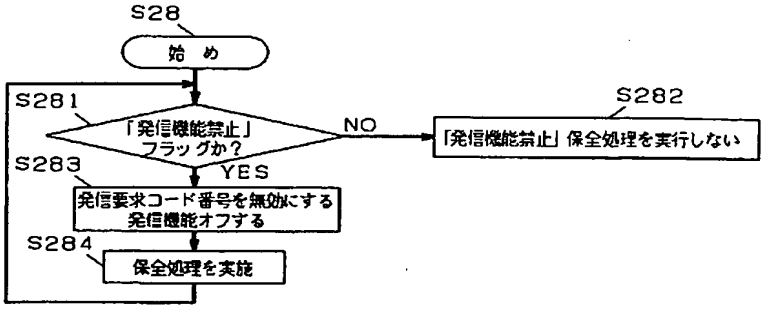
【図４】



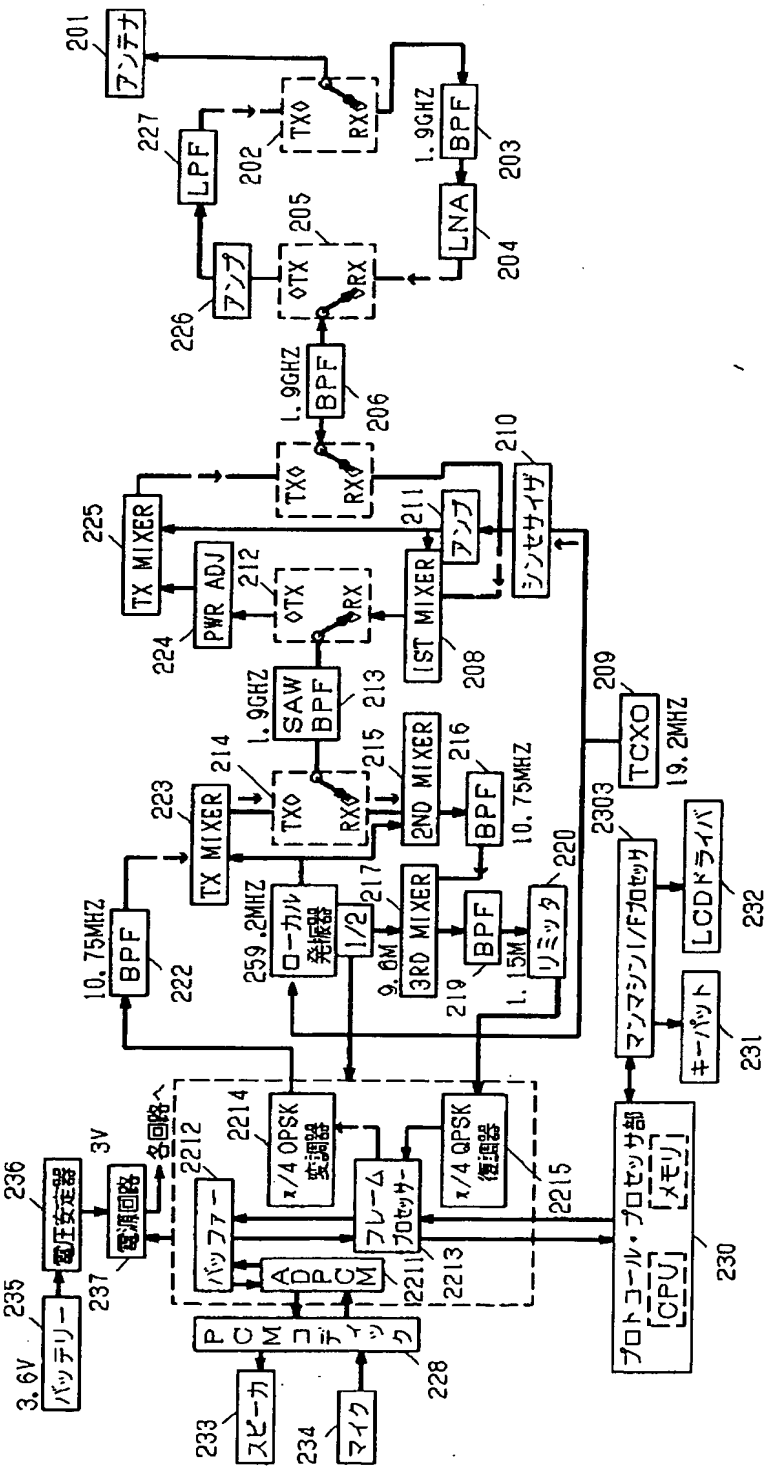
【図１７】



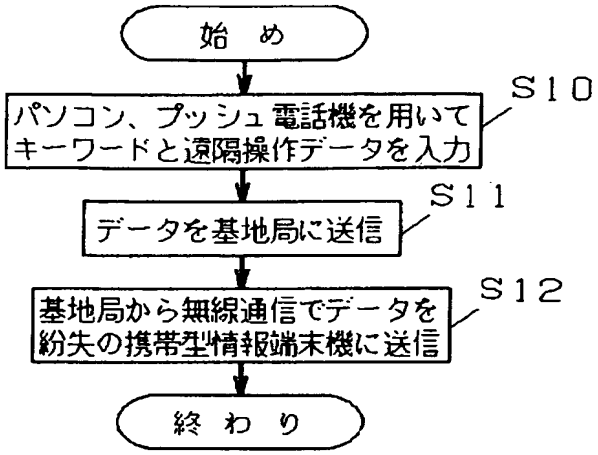
【図１１】



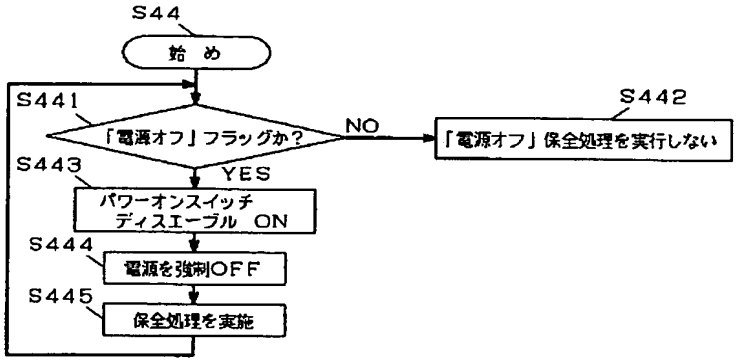
【図２】


201
アンテナ
227
LPF
202
TXΦ
RXΦ
1.9GHZ
BPF
203
LNA
204
205
ΦTX
RX
226
アンプ
1.9GHZ
BPF
206
TXΦ
RXΦ
210
シンセサイザ
225
TX MIXER
211
アンプ
224
PWR ADJ
212
ΦTX
ΦRX
1ST MIXER
208
1.9GHZ
SAW
BPF
213
209
TCXO
19.2MHZ
223
TX MIXER
214
TXΦ
RXΦ
215
2ND MIXER
216
BPF
10.75MHZ
2303
220
リミッタ
10.75MHZ
BPF
222
259.2MHZ
ローカル
発振器
1/2
217
9.0M
3RD MIXER
219
BPF
1.15M
LCDドライバ
232
マンマシンI/Fプロセッサ
キーパット
231
236
電圧安定器
3V
各回路へ
電源回路
2212
2214
π/4 QPSK
変調器
π/4 QPSK
復調器
2215
バッファー
フレーム
プロセッサー
プロトコール・プロセッサ部
CPU
メモリ
230
235
3.6V
バッテリー
237
ADPCM
2211
2213
PCMコーデック
228
233
スピーカ
234
マイク

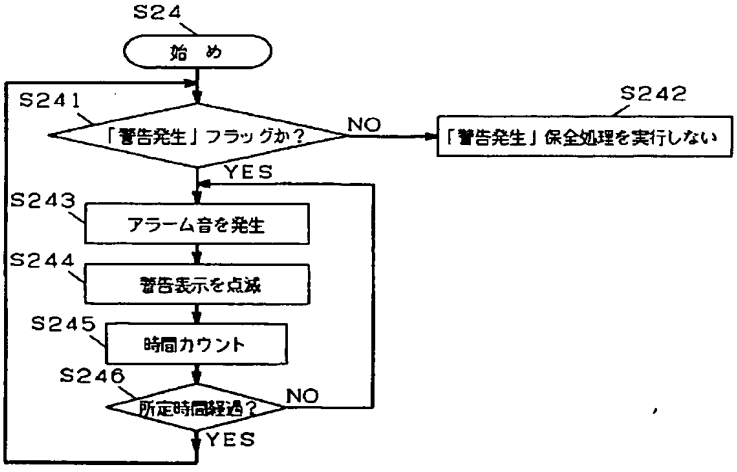
【図５】


始　め
パソコン、プッシュ電話機を用いて
キーワードと遠隔操作データを入力
S10
データを基地局に送信
S11
基地局から無線通信でデータを
紛失の携帯型情報端末機に送信
S12
終　わ　り

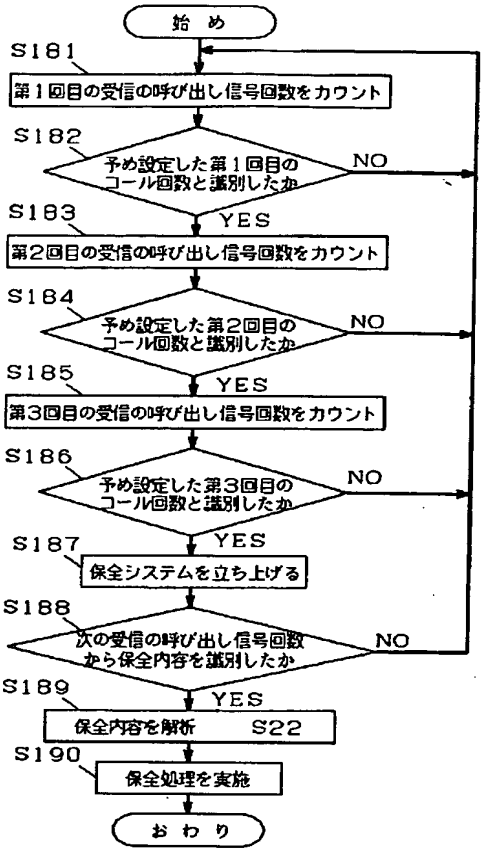
【図７】


S44
始　め
S441
「電源オフ」フラグか？
NO
S442
「電源オフ」保全処理を実行しない
YES
S443
パワーオンスイッチ
ディスエーブル　ON
S444
電源を強制OFF
S445
保全処理を実施

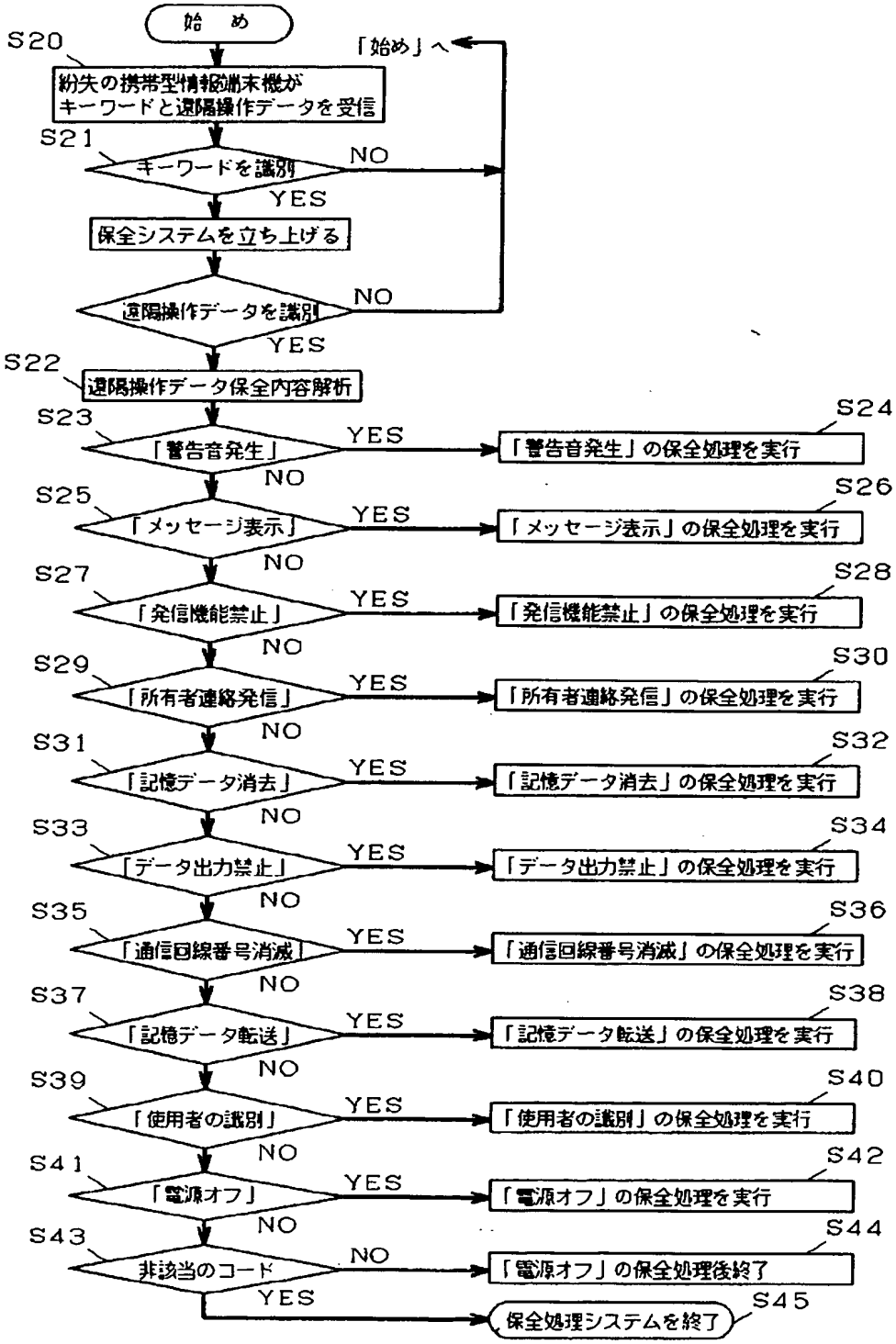
【図８】


S24
始　め
S241
「警告発生」フラグか？
NO
S242
「警告発生」保全処理を実行しない
YES
S243
アラーム音を発生
S244
警告表示を点滅
S245
時間カウント
S246
所定時間経過？
NO
YES

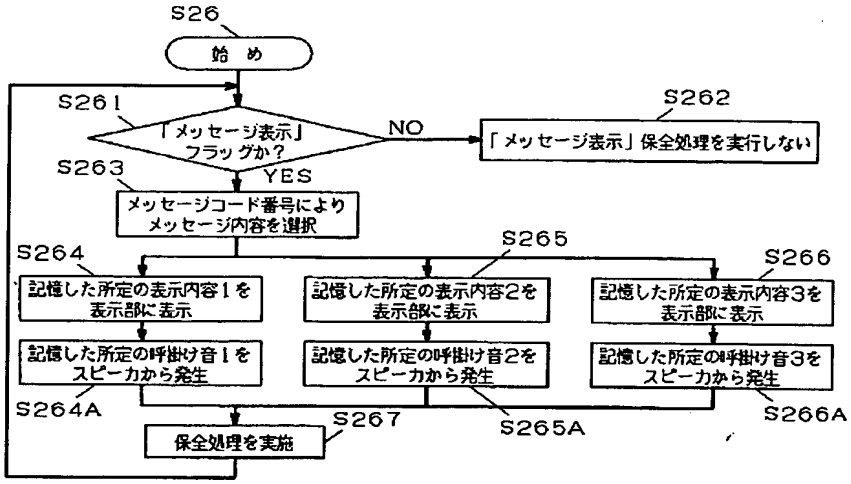
【図１８】


始　め
S181
第１回目の受信の呼び出し信号回数をカウント
S182
予め設定した第１回目の
コール回数と識別したか
NO
YES
S183
第２回目の受信の呼び出し信号回数をカウント
S184
予め設定した第２回目の
コール回数と識別したか
NO
YES
S185
第３回目の受信の呼び出し信号回数をカウント
S186
予め設定した第３回目の
コール回数と識別したか
NO
YES
S187
保全システムを立ち上げる
S188
次の受信の呼び出し信号回数
から保全内容を識別したか
NO
YES
S189
保全内容を解析　S22
S190
保全処理を実施
おわり

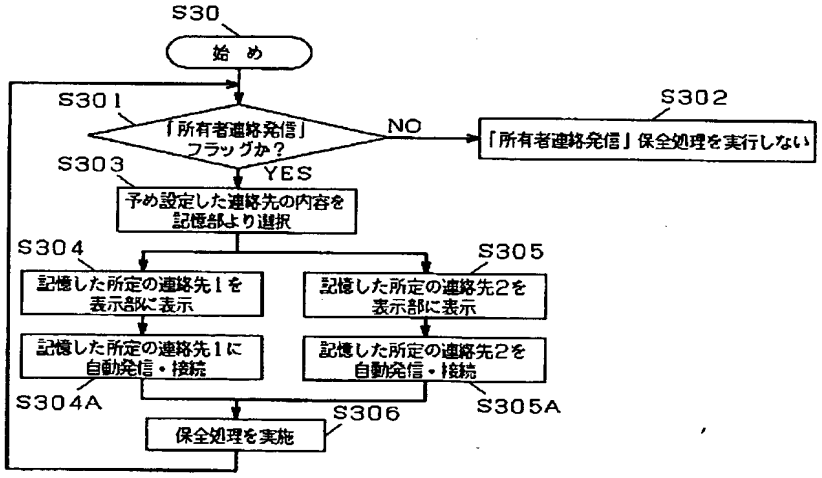
【図６】


始　め
S20
紛失の携帯型情報端末機が
キーワードと遠隔操作データを受信
「始め」へ
S21
キーワードを識別
NO
YES
保全システムを立ち上げる
遠隔操作データを識別
NO
YES
S22
遠隔操作データ保全内容解析
S23
「警告音発生」
YES
S24
「警告音発生」の保全処理を実行
NO
S25
「メッセージ表示」
YES
S26
「メッセージ表示」の保全処理を実行
NO
S27
「発信機能禁止」
YES
S28
「発信機能禁止」の保全処理を実行
NO
S29
「所有者連絡発信」
YES
S30
「所有者連絡発信」の保全処理を実行
NO
S31
「記憶データ消去」
YES
S32
「記憶データ消去」の保全処理を実行
NO
S33
「データ出力禁止」
YES
S34
「データ出力禁止」の保全処理を実行
NO
S35
「通信回線番号消滅」
YES
S36
「通信回線番号消滅」の保全処理を実行
NO
S37
「記憶データ転送」
YES
S38
「記憶データ転送」の保全処理を実行
NO
S39
「使用者の識別」
YES
S40
「使用者の識別」の保全処理を実行
NO
S41
「電源オフ」
YES
S42
「電源オフ」の保全処理を実行
NO
S43
非該当のコード
NO
S44
「電源オフ」の保全処理後終了
YES
S45
保全処理システムを終了

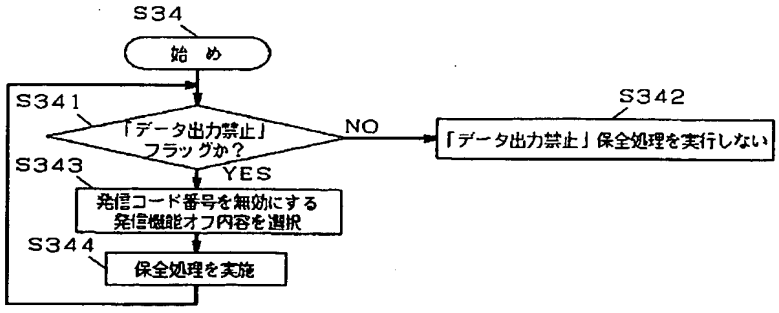
【図９】


S26
始 め
S261
「メッセージ表示」フラッグか？
NO
S262
「メッセージ表示」保全処理を実行しない
YES
S263
メッセージコード番号によりメッセージ内容を選択
S264
S265
S266
記憶した所定の表示内容1を表示部に表示
記憶した所定の表示内容2を表示部に表示
記憶した所定の表示内容3を表示部に表示
記憶した所定の呼出け音1をスピーカから発生
記憶した所定の呼出け音2をスピーカから発生
記憶した所定の呼出け音3をスピーカから発生
S264A
S265A
S266A
S267
保全処理を実施

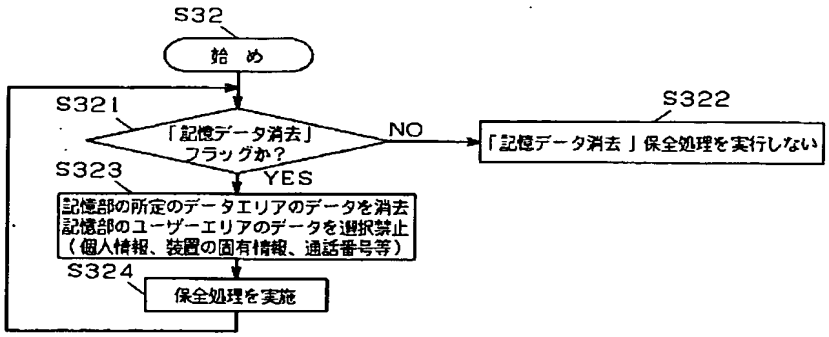
【図１０】


S30
始 め
S301
「所有者連絡発信」フラッグか？
NO
S302
「所有者連絡発信」保全処理を実行しない
YES
S303
予め設定した連絡先の内容を記憶部より選択
S304
S305
記憶した所定の連絡先1を表示部に表示
記憶した所定の連絡先2を表示部に表示
記憶した所定の連絡先1に自動発信・接続
記憶した所定の連絡先2を自動発信・接続
S304A
S305A
S306
保全処理を実施

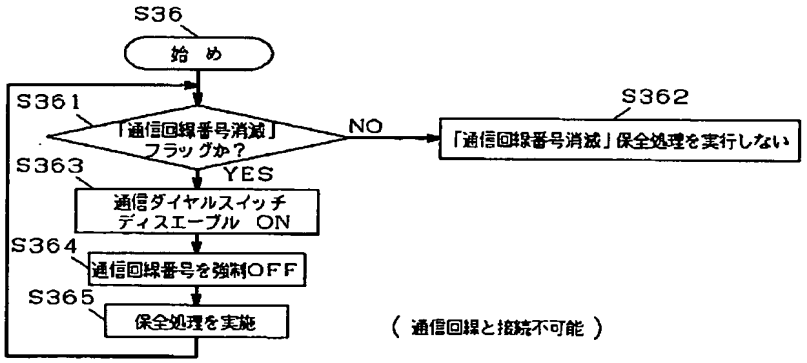
【図１２】


S34
始 め
S341
「データ出力禁止」フラッグか？
NO
S342
「データ出力禁止」保全処理を実行しない
YES
S343
発信コード番号を無効にする発信機能オフ内容を選択
S344
保全処理を実施

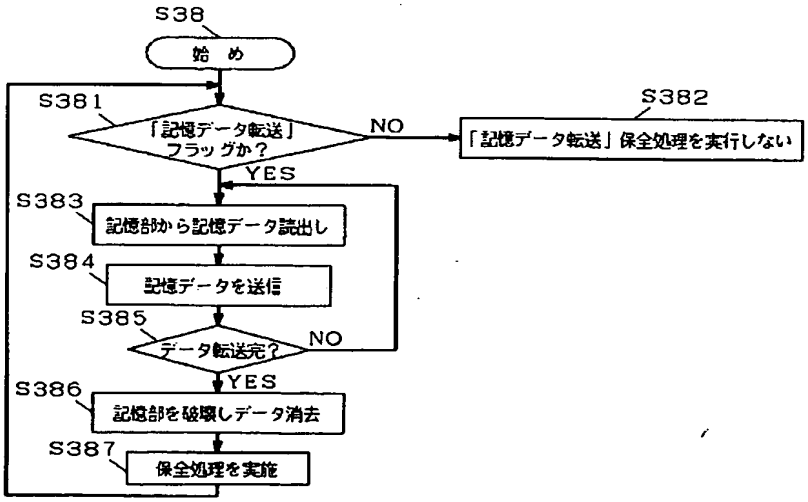
【図１３】


S32
始 め
S321
「記憶データ消去」フラッグか？
NO
S322
「記憶データ消去」保全処理を実行しない
YES
S323
記憶部の所定のデータエリアのデータを消去
記憶部のユーザーエリアのデータを選択禁止
（個人情報、装置の固有情報、通話番号等）
S324
保全処理を実施

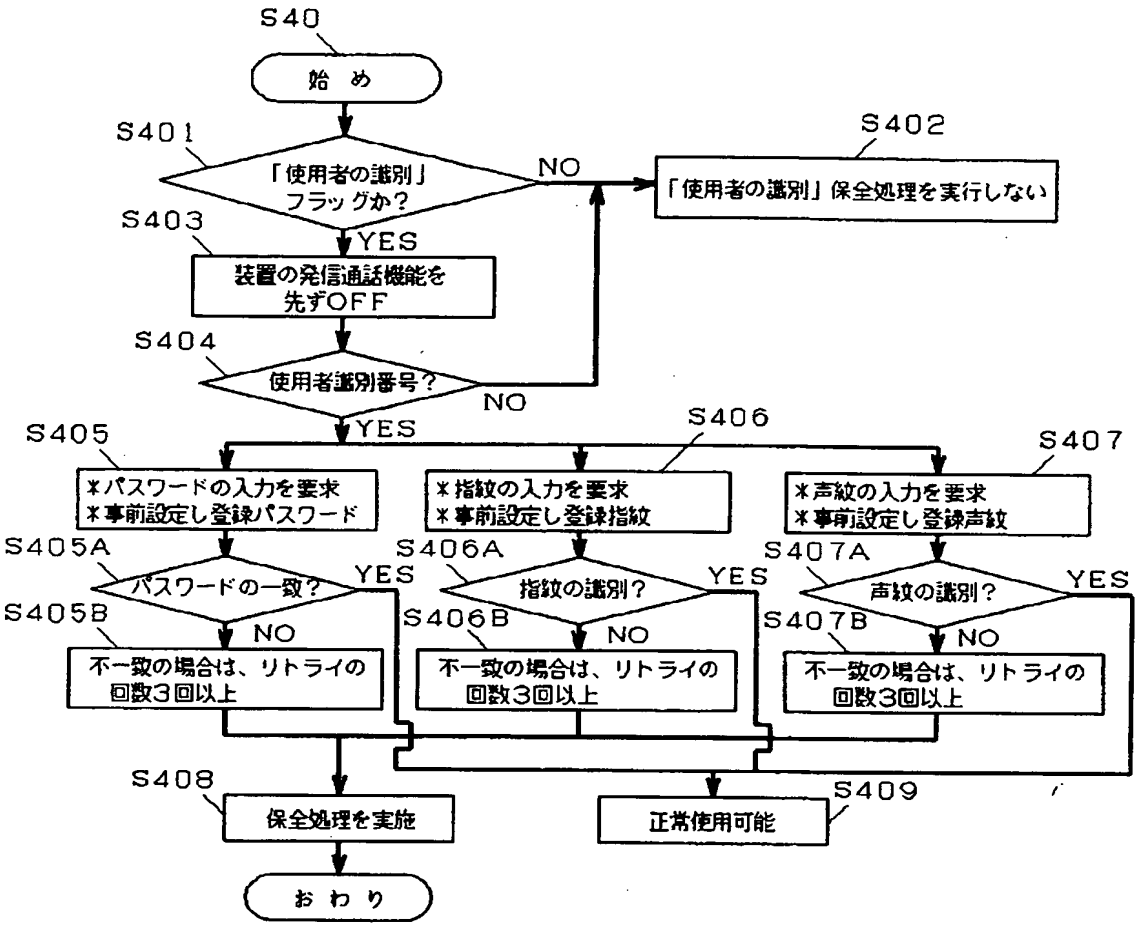
【図１４】


S36
始 め
S361
「通信回線番号消滅」フラッグか？
NO
S362
「通信回線番号消滅」保全処理を実行しない
YES
S363
通信ダイヤルスイッチ
ディスエーブル ON
S364
通信回線番号を強制OFF
S365
保全処理を実施
（通信回線と接続不可能）

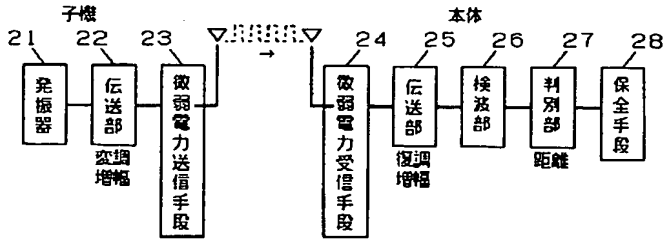
【図１５】


S38
始 め
S381
「記憶データ転送」フラッグか？
NO
S382
「記憶データ転送」保全処理を実行しない
YES
S383
記憶部から記憶データ読出し
S384
記憶データを送信
S385
データ転送完？
NO
YES
S386
記憶部を破壊しデータ消去
S387
保全処理を実施

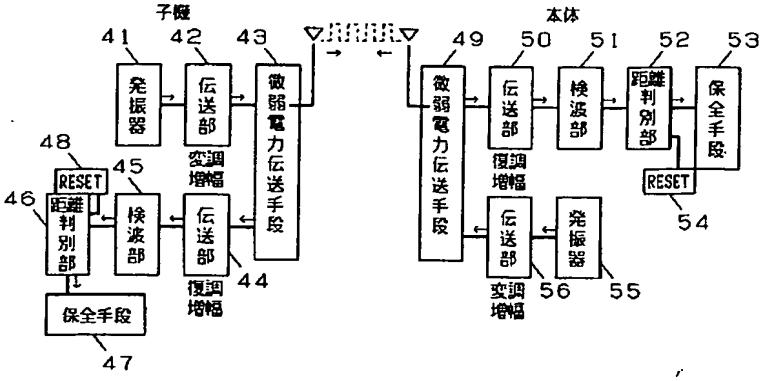
【図１６】


S40
始 め
S401
「使用者の識別」フラッグか?
NO
S402
「使用者の識別」保全処理を実行しない
YES
S403
装置の発信通話機能を先ずOFF
S404
使用者識別番号?
NO
YES
S405
S406
S407
＊パスワードの入力を要求
＊事前設定し登録パスワード
＊指紋の入力を要求
＊事前設定し登録指紋
＊声紋の入力を要求
＊事前設定し登録声紋
S405A
パスワードの一致?
YES
S406A
指紋の識別?
YES
S407A
声紋の識別?
YES
S405B
NO
不一致の場合は、リトライの回数3回以上
S406B
NO
不一致の場合は、リトライの回数3回以上
S407B
NO
不一致の場合は、リトライの回数3回以上
S408
保全処理を実施
S409
正常使用可能
お わ り

【図１９】


子機
本体
21
22
23
24
25
26
27
28
発振器
伝送部
変調増幅
微弱電力送信手段
微弱電力受信手段
伝送部
復調増幅
検波部
判別部
距離
保全手段

【図２０】


子機
本体
41
42
43
49
50
51
52
53
発振器
伝送部
変調増幅
微弱電力伝送手段
微弱電力伝送手段
伝送部
復調増幅
検波部
距離判別部
保全手段
RESET
54
48
45
46
RESET
距離判別部
検波部
伝送部
復調増幅
44
伝送部
変調増幅
56
発振器
55
保全手段
47

Japanese Patent Application, Laid-Open Publication No. H10-177525

INT. CL.[6]: G06F 12/14
G08B 25/10
H04Q 7/38

PUBLICATION DATE: June 30, 1998

TITLE Portable Electronic Device Protection System

APPLICATION NO. H8-335336

FILING DATE December 16, 1996

APPLICANT(S) MATSUSHITA ELECTRIC INDUSTRIES CO., LTD.

INVENTOR(S) Fusaki MIURA

ABSTRACT

PROBLEM To prevent owners or transmission partners of lost or stolen portable electronic devices from suffering damages.

SOLUTION A portable electronic device comprises a receiving portion 11 for receiving remote operation data transmitted through signal transmitting means, an identifying portion 12 for identifying remote operation data received at the receiving portion 11 and a predetermined protecting portion 13 for eliminating damage to the owner of the portable electronic device based on the identification results of the identifying portion 12, wherein a protection procedure is performed by the protecting portion 13 before contacting a network or online system line business company to cancel the line when the portable electronic device 1 is lost or stolen, thereby enabling security relating to property or information of the owner of the portable electronic device to be increased.

CLAIMS

1. A portable electronic device protecting system characterized by comprising receiving means for receiving remote operation data transmitted to the portable electronic device through signal transmitting means, identifying means for identifying the remote operation data received by said receiving means, and protection processing means for eliminating damage suffered by the owner of the portable electronic device based on identification results due to said identifying means, thereby increasing the security of property or information of the owner of the portable electronic device.

2. A portable electronic device protecting system as recited in claim 1, characterized by comprising protection processing means for increasing predetermined security to eliminate damage

suffered by the owner of the portable electronic device due to the identification results of remote operation data sent through the signal transmitting means when the portable electronic device is lost or stolen.

3. A portable electronic device protecting system as recited in claim 2, characterized by comprising one or more protection processing means for receiving remote operation data transmitted through the signal transmitting means and eliminating damage suffered to partners to whom the owner of the portable electronic device and partner information due to the identification results of said remote operation data.

4. A portable electronic device protecting system as recited in claim 2 or 3, characterized in that the protection processing means comprises first memory means for storing key words pre-inputted by the owner of the portable electronic device and second memory means for receiving remote operation data transmitted through the signal communication means and recording key word information of the identification results of said remote operation data, wherein the protection procedure is performed after confirming that the key word of said first memory means and the key word information of said second memory means match.

5. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of turning the power off is performed, whereby the original functions of the portable electronic device are suspended and made unusable to others aside from the owner of the lost or stolen portable electronic device when the others attempt to use it.

6. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of emitting a warning is performed, whereby an audio or visual alarm is emitted and use is prohibited when others aside from the owner of the lost or stolen portable electronic device attempt to use it.

7. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of displaying a message is performed, whereby a contact address or message pre-inputted by the owner and stored in the memory means is displayed to recover the portable electronic device when others aside from the owner of the lost or stolen portable electronic device attempt to use it.

8. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of contacting the owner is performed, whereby the original functions are suspended and a contact address

pre-inputted by the owner and stored in the memory means is contacted when others aside from the owner of the lost or stolen portable electronic device attempt to use it.

9. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of prohibiting calling functions is performed, whereby functions pre-inputted by the owner among the original functions of the lost or stolen portable electronic device are suspended.

10. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of prohibiting data output is performed, whereby the outputting of data from the memory means of the lost or stolen portable electronic device is prohibited.

11. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of deleting memory data is performed, whereby the data in the memory means of the lost or stolen portable electronic device is deleted so as to keep it from being seen or used by others.

12. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of canceling the communication line number is performed, whereby the communication line number of the lost or stolen portable electronic device is canceled so as to make it unusable to others.

13. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, the protection process of transferring memory data is performed, whereby the data of the memory means of the lost or stolen portable electronic device is transferred to another predetermined electronic device to recovery the memory data.

14. A portable electronic device protecting system as recited in claim 3, characterized in that as the content of the protection processing of the protection processing means, a security process of identifying the user by means of a user identification means and making it impossible for others aside form the owner to use the portable electronic device is performed.

15. A portable electronic device protecting system as recited in claim 3, characterized in that with respect to a transmission partner or partner information, the protection processing means, due to remote operation data, performs at least one process among:

a. a protection process for transmitting to partners to which transmissions have been made with the portable electronic device predetermined information that the owner is under circumstances of not

being able to receive,

b. a protection process for suspending a function of receiving information from partners to which transmission have been made with the portable electronic device,

c. a protection process for transmitting data being communicated or used to partners to which transmissions have been made with the portable electronic device,

d. a protection process for suspending a function of transmitting transmitted information to partners to which transmissions have been made with the portable electronic device,

e. a protection process for transmitting a lost message pre-inputted by the owner and stored in the memory means to partners to which transmissions have been made with the portable electronic device, and

f. a protection process for preventing use of the portable electronic device protecting system to partners to which transmissions have been made with the portable electronic device.

16. A portable electronic device protecting system as recited in any one of claims 5-14, characterized in that when signal communication means are used as a transmission medium to receive a key word signal pre-inputted by the owner and stored in the memory means, the protection processing means of the portable electronic device is forcibly driven as a result of identification results of remote operation data, to perform a protection process of increasing predetermined security to eliminate damage suffered by the owner.

17. A portable electronic device protecting system as recited in any one of claims 5-14, characterized in that when a pattern of a callup signal number pre-inputted by the owner and stored in the memory means is received, the protection processing means of the portable electronic device is forcibly driven as a result of identification results of remote operation data, to perform a protection process of increasing predetermined security to eliminate damage suffered by the owner.

18. A portable electronic device protecting system, characterized by having a sub-device comprising oscillating means for prompting a protection process in the portable electronic device, and low-power transmitting means for transmitting an oscillation signal of said oscillating means, and a main device comprising low-power receiving means for receiving oscillation data for prompting protection processes from said sub-device, identifying means for identifying operation data received by said low-power receiving means and predetermined protection means for eliminating damage suffered by the owner of the portable electronic device by means of identification results of said identifying means, thereby increasing the security relating to the property or information of the owner of the portable electronic device.

19. A portable electronic device protecting system characterized by comprising a portable electronic device sub device having low-power transmitting means for exchanging signals with the

portable electronic device, determining means for determining the distance between a received signal of said low-power transmitting means and the portable electronic device, and means for generating a warning tone due to oscillation data upon receiving said oscillation data by said low-power transmitting means for prompting a protection process due to a determination result of the determination means that it is separated by more than a predetermined distance, and a main device having bi-directional low-power transmitting means similar to that of said sub device, determining means for determining the distance from the sub device, and means for generating a warning tone by activating the protection process due to the determination result of said determining means of being separated by more than a predetermined distance, thereby preventing loss or theft and misplacement.

DETAILED DESCRIPTION OF THE INVENTION

Field of Industrial Application

The present invention relates to a portable electronic device protecting system provided with a protection processing function for increasing a predetermined level of security by eliminating damage suffered by an owner with respect to a stolen or lost portable electronic device (referring to data processing terminal devices having signal communicating means including PHS and cellular telephones).

Conventional Art

Conventionally, portable electronic devices such as described above are used by carrying them outdoors over a wide and unspecified region due to the properties of these devices. Additionally, the uses of portable electronic devices are expanding with PHS (Personal Handy Phone System) and computer peripheral terminal devices for digital signal information such as data processing terminal devices thereof, thus enabling their range of carrying and use to be further expanded. Additionally, their method of use is simple, with demand coming from a large number of people.

Problems to be Solved by the Invention

However, these conventional types of portable electronic devices are used by the owner by carrying the devices themselves outdoors, and are readily carried, thus having many opportunities for being stolen or lost, and when this type of lost or stolen portable electronic device is picked up by another, it is likely to be easily used, so that the original owner may suffer damage such as having private information or important data seen or be required to pay communication fees for calls which have been made by another.

Additionally, the partners of transmission by the owner of a lost or stolen portable electronic device also risk suffering damage due to sending transmissions to the owner of the portable electronic device without knowing that the conditions are not satisfactory.

The present invention has the object of offering a portable electronic device protecting system for resolving the above-described conventional problems, by eliminating damage suffered by owners and transmission partners of lost or stolen portable electronic devices.

Means for Solving the Problems

In order to resolve these problems, the present invention comprises comprising receiving means for

receiving remote operation data transmitted to the portable electronic device through signal transmitting means, identifying means for identifying the remote operation data received by said receiving means, and protection processing means for eliminating damage suffered by the owner of the portable electronic device based on identification results due to said identifying means.

As a result, it is possible to eliminate damage suffered by owners or communication partners of lost or stolen portable electronic devices.

Embodiments of the Invention

The invention recited in claim 1 of the present invention comprises receiving means for receiving remote operation data transmitted to the portable electronic device through signal transmitting means, identifying means for identifying the remote operation data received by said receiving means, and protection processing means for eliminating damage suffered by the owner of the portable electronic device based on identification results due to said identifying means, thus enabling damage suffered by the owner or communication partner of the lost or stolen portable electronic device to be eliminated and increasing security relating to property or information of the owner of the portable electronic device.

The invention recited in claim 2 of the present invention comprises protection processing means for increasing predetermined security to eliminate damage suffered by the owner of the portable electronic device due to the identification results of remote operation data sent through the signal transmitting means when the portable electronic device is lost or stolen, thus enabling damage suffered by the owner or communication partner of the lost or stolen portable electronic device to be eliminated and increasing security relating to property or information of the owner of the portable electronic device.

The invention recited in claim 3 of the present invention comprises one or more protection processing means for receiving remote operation data transmitted through the signal transmitting means and eliminating damage suffered to partners to whom the owner of the portable electronic device and partner information due to the identification results of said remote operation data, thus enabling damage suffered by the owner or communication partner of the lost or stolen portable electronic device to be eliminated and increasing security relating to property or information of the owner of the portable electronic device.

The invention recited in claim 4 of the present invention is such that the protection processing means comprises first memory means for storing key words pre-inputted by the owner of the portable electronic device and second memory means for receiving remote operation data transmitted through the signal communication means and recording key word information of the identification results of said remote operation data, wherein the protection procedure is performed after confirming that the key word of said first memory means and the key word information of said second memory means match, so that the respective key words must be inputted each time the portable electronic device is used or it will not work, thereby maintaining a level of security that ensures protection, safety and reliability of important registration information of the owner, achieving a system that offers strict protection due to application of separate key words, and avoiding the occurrence of errors in the control work in the case of loss or theft to increase the level of security of the registration information and its control.

The invention recited in claim 5 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of turning the power off is performed, whereby the original functions of the portable electronic device are suspended and made unusable to others aside from the owner of the lost or stolen portable electronic device when the others attempt to use it, thus achieving a protection process of canceling the basic functions of the portable electronic device by turning off the power, thus holding the loss to the one losing the portable electronic device to a minimum.

The invention recited in claim 6 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of emitting a warning is performed,

whereby an audio or visual alarm is emitted and use is prohibited when others aside from the owner of the lost or stolen portable electronic device attempt to use it, thereby enabling a protection process of prohibiting use of the portable electronic device by issuing a warning to the finder of the portable electronic device, thus preventing others aside from the one losing the portable electronic device from using it.

The invention recited in claim 7 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of displaying a message is performed, whereby a contact address or message pre-inputted by the owner and stored in the memory means is displayed to recover the portable electronic device when others aside from the owner of the lost or stolen portable electronic device attempt to use it, thereby enabling a protection process of requesting return of the portable electronic device, thereby preventing use by others aside from the one losing the portable electronic device and making return of the portable electronic device possible.

The invention recited in claim 8 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of contacting the owner is performed, whereby the original functions are suspended and a contact address pre-inputted by the owner and stored in the memory means is contacted when others aside from the owner of the lost or stolen portable electronic device attempt to use it, thus enabling contact to be achieved by issuing a signal to contact the owner when the finder of the portable electronic device uses it, thereby preventing use by others aside from the one losing the portable electronic device and enabling the portable electronic device to be returned.

The invention recited in claim 9 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of prohibiting calling functions is performed, whereby functions pre-inputted by the owner among the original functions of the lost or stolen portable electronic device are suspended, thereby enabling use by others aside from the one losing the portable electronic device to be prevented, and avoiding fees incurred on invalid use.

The invention recited in claim 10 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of prohibiting data output is performed, whereby the outputting of data from the memory means of the lost or stolen portable electronic device is prohibited, thereby enabling use by others aside from the one losing the portable electronic device to be prevented, and avoiding fees incurred on invalid use.

The invention recited in claim 11 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of deleting memory data is performed, whereby the data in the memory means of the lost or stolen portable electronic device is deleted so as to keep it from being seen or used by others, thereby enabling memory data protecting personal data or information inside the portable electronic device to be deleted, thus preventing use by others aside from the one losing the portable electronic device, avoiding fees being incurred on invalid use, and preventing misuse of the personal data and information.

The invention recited in claim 12 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of canceling the communication line number is performed, whereby the communication line number of the lost or stolen portable electronic device is canceled so as to make it unusable to others, thereby enabling the communication line number to be deleted against use by the finder of the portable electronic device, enabling use by others aside from the one losing the portable electronic device to be prevented, and avoiding fees incurred on invalid use.

The invention recited in claim 13 of the present invention is such that as the content of the protection processing of the protection processing means, the protection process of transferring memory data is performed, whereby the data of the memory means of the lost or stolen portable electronic device is

transferred to another predetermined electronic device to recovery the memory data, thereby enabling data transfer of personal data and information inside the portable electronic device by remote operation to recover the personal data and information inside the portable electronic device, enabling the memory data inside the portable electronic device to be deleted, enabling use by others aside from the one losing the portable electronic device to be prevented, and avoiding fees incurred on invalid use.

The invention recited in claim 14 of the present invention is such that as the content of the protection processing of the protection processing means, a security process of identifying the user by means of a user identification means and making it impossible for others aside form the owner to use the portable electronic device is performed, thereby enabling increase to a predetermined security level by protecting personal data inside the portable electronic device and preventing use by others even if the portable electronic device is lost or stolen.

The invention recited in claim 15 of the present invention is such that with respect to a transmission partner or partner information, the protection processing means, due to remote operation data, performs at least one process among: a. a protection process for transmitting to partners to which transmissions have been made with the portable electronic device predetermined information that the owner is under circumstances of not being able to receive, b. a protection process for suspending a function of receiving information from partners to which transmission have been made with the portable electronic device, c. a protection process for transmitting data being communicated or used to partners to which transmissions have been made with the portable electronic device, d. a protection process for suspending a function of transmitting transmitted information to partners to which transmissions have been made with the portable electronic device, e. a protection process for transmitting a lost message pre-inputted by the owner and stored in the memory means to partners to which transmissions have been made with the portable electronic device, and f. a protection process for preventing use of the portable electronic device protecting system to partners to which transmissions have been made with the portable electronic device, so that when the portable electronic device is lost or stolen, the owner of the portable electronic device protecting system can store a pre-inputted key word, which key word data can be transmitted to another transmitting device by remote operation with radio communications as the medium, such that after confirming a match of the key word information, the protection process can be run, so as to maintain security to ensure protection, safety and reliability of registration information important to the owner, thereby avoiding the danger of misuse by others even when lost or stolen.

The invention recited in claim 16 of the present invention is such that when signal communication means are used as a transmission medium to receive a key word signal pre-inputted by the owner and stored in the memory means, the protection processing means of the portable electronic device is forcibly driven as a result of identification results of remote operation data, to perform a protection process of increasing predetermined security to eliminate damage suffered by the owner, so that due to the one losing the portable electronic device having pre-inputted and stored in the memory means a key word signal, the protection function of the portable electronic device is forcibly activated to prevent use by others aside from the one losing the device.

The invention recited in claim 17 of the present invention is such that when a pattern of a callup signal number pre-inputted by the owner and stored in the memory means is received, the protection processing means of the portable electronic device is forcibly driven as a result of identification results of remote operation data, to perform a protection process of increasing predetermined security to eliminate damage suffered by the owner, so that even when the finder of the portable electronic device does not reply or cannot communicate, a remote protection procedure due to a pattern of a callup signal number can be activated to prevent use by others aside from the one losing the device.

The invention recited in claim 18 of the present invention comprises a sub-device comprising oscillating means for prompting a protection process in the portable electronic device, and low-power transmitting means for transmitting an oscillation signal of said oscillating means, and a main device comprising low-power receiving means for receiving oscillation data for prompting protection processes from said sub-

device, identifying means for identifying operation data received by said low-power receiving means and predetermined protection means for eliminating damage suffered by the owner of the portable electronic device by means of identification results of said identifying means, thereby increasing the security relating to the property or information of the owner of the portable electronic device, thus enabling loss or misplacement to be prevented and avoided before it happens, and even if the owner loses or forgets the portable electronic device, automatically activating various types of protection functions for prompting protection procedures in the main device, to readily increase the security relating to property or information of the owner of the device even if found by another.

The invention as recited in claim 19 of the present invention comprises a portable electronic device sub device having low-power transmitting means for exchanging signals with the portable electronic device, determining means for determining the distance between a received signal of said low-power transmitting means and the portable electronic device, and means for generating a warning tone due to oscillation data upon receiving said oscillation data by said low-power transmitting means for prompting a protection process due to a determination result of the determination means that it is separated by more than a predetermined distance, and a main device having bi-directional low-power transmitting means similar to that of said sub device, determining means for determining the distance from the sub device, and means for generating a warning tone by activating the protection process due to the determination result of said determining means of being separated by more than a predetermined distance, thereby preventing loss or theft and misplacement, thereby readily achieving a portable electronic device protecting system for preventing loss or misplacement of the portable electronic device, and preventing loss or misplacement of the portable electronic device.

Herebelow, embodiments of the present invention shall be described with reference to the drawings.

(Embodiment 1)

Fig. 1 is a structural diagram of a portable electronic device protecting system according to Embodiment 1 corresponding to claim 1 of the present invention. In the drawing, 1 denotes a portable electronic device such as a PHS (Personal Handy Phone System) data communication device or portable telephone, 2a, 2b and 2c denote radio communication means such as a communication channel connected to a public line network, 3 denotes a telephone such as a PHS as a portable telephone or a common public telephone connected to a public line network, and 4 denotes a relay base station. Furthermore, the telephone 3A also forms a separate PHS as a portable telephone or PHS data communication terminal through the radio communication line 2b connected to the public line network or the like.

The portable electronic device 1 comprises a receiving portion 11 for receiving remote operation data with radio signal communication means 2a as the transmission medium, an identifying portion 12 for identifying received remote operation data, and a predetermined protecting portion 13 for eliminating damage suffered by the owner of the portable electronic device due to the results of the identification by the identifying portion 12, and performs security relating to property or information of the owner of the portable electronic device 1, and protects property or information of the owner of the portable electronic device.

Remote operation data are sent from the PHS 3A as a PHS data communication device or portable telephone to a portable electronic device requiring protection through a radio communication line 2c, or from a common public telephone 3 inside or outside a metropolitan area through the public line network 2b. The portable electronic device 1 receives said remote operation data with the receiving portion 11, and the identifying portion 12 determines whether the received remote operation data matches with predetermined remote operation data which has been previously stored. The protecting portion 13 performs a predetermined protecting process to eliminate damage suffered by the owner of the portable electronic device 1 only if the results of the determination in the identifying portion 12 confirm a match.

Next, Fig. 4 is a structural diagram showing a portable electronic device network system, wherein

common telephones 31 are connected to a public and dedicated line network 30 through an exchange, along with a personal computer 32 with a modulator-demodulator (modem), a number of portable electronic device base stations 33-35 and a network control station 36. The number of base stations 33-35 each has a portable electronic device connected through a radio communication line. For example, a portable type personal computer, radio communication personal computer and radio communication electronic notebook are connected to the base station 33 through the radio communication line, a portable telephone, PHS and radio communicator are connected to the base station 34 through a radio communication line, and a portable information terminal is connected to the base station 35 through a radio communication line. Additionally, the network control station 36 controls and manages the entire network, and controls each terminal.

Each portable electronic device has a protection function, these protection functions, upon receiving remote operation data sent from the owner, performing control to run predetermined protection processes for eliminating potential causes of problems to the owner of a portable electronic device based on the remote operation data, control for performing analysis procedures or input of key words, and control for performing protection procedures set with respect to different inputs as well.

Thus, in Embodiment 1 of the present invention, the remote electronic device has the effect of being able to increase security relating to property or information of the owner of the portable electronic device by means of a receiving portion 11 for remote operation data through the radio signal communicating means and a transmission medium, an identifying portion 12 for identifying received remote operation data, and a protecting portion 13 for eliminating damage suffered by the owner of a portable electronic device due to the results of the identification of the identifying portion 12.

(Embodiment 2)

Fig. 2 is a functional block diagram of, for example, a PHS terminal showing the structure of a portable electronic device protecting system according to Embodiment 2 corresponding to claim 2 of the present invention, composed of a key panel and an RF panel. In the drawing, the modem portion 221 comprises an ADPCM codec 2211 for compressing and expanding an audio code by adaptive prediction and adaptive quantization, a buffer 2212, a frame processor 2213, a /4QPSK modulator 2214 and a /4 QPSK demodulator 2215, with a speaker 233 and microphone 234 being connected to the ADPCM codec 2211 through a PCM codec 228. Additionally, 235 denotes a battery, 236 denotes a voltage stabilizer and 237 denotes a power supply circuit for supplying electrical power to the respective circuits.

The protocol processor portion 230 is for controlling the portable electronic device in accordance with a predetermined protocol, and is composed of a CPU and memory and the like. Fig. 3 shows the structure of a protocol processor portion. In the drawing, the protocol processor portion 230 comprises a CPU (control portion) 2301, a protocol processor 2302, a man-machine I/F processor 2302 for a calendar watch, touch panel, display portion I/F, infrared I/F, serial I/F, PC card I/F, audio generating I/F, various types of sensor I/F and various types of input I/F, a memory 2304 such as a RAM, ROM or F-ROM, a protection processing portion 2305, a protocol processor 2306 for activating a calling function, a transmitting function and a transfer function, an RF controller 2307 and a power control portion 2308, with a keypad 231 and LCD drive 232 being connected to the man-machine I/F processor 2303.

In this structure, the radio transmitting-receiving portion sends radio signals arriving at the antenna 201 through the FET switch 202 for switching between transmitting and receiving selected to the receiving side, and after they are selected by the bandpass filter (BPF) 203 in the receiving band, are amplified by the LNA (low noise amp) 204. This LNA 204 contains an internal attenuator, so that when inputting signals with a strong electric field, switching over to the attenuator prevents saturation of the receiving circuit to obtain a wide dynamic range. The signals amplified by the LNA 204 are sent through the transmission-reception switching FET switch 205, through another bandpass filter (BPF) 206, and after deleting unneeded signals such as images in the BPF 206, sent through the transmission-reception switching FET switch 207 to the first mixer 208.

At the first mixer 208, the received signal is mixed with a first local signal obtained by passing an oscillation signal of the oscillating portion (TCXO) from the synthesizer 210 to the amp 211, thus selecting a frequency channel and converting to the intermediate frequency of 248.45 MHz. In order to increase the property of withstanding disturbances due to intermodulation, a high intercept point is used. The output of the mixer 208 is outputted via the transmission-reception switching FET switch 212 through the SAW filter (BPF) 213 having a narrow-band filter property. This SAW filter 213 determines the selectivity of the adjacent channels and image disturbance properties, and simultaneously has excellent group delay properties. When using a helical filter for analog cordless as a substitute for the SAW filter, only the image frequency is attenuated, and deletion is performed in the intermediate frequency which is the next stage.

The signal which has passed through the SAW filter 213 is inputted via the transmission-reception switching FET switch 214 to the second mixer 215, and mixed with a signal form the local oscillator 218 and converted to 10.75 MHz. Since the second image disturbance is decided only by the function of the SAW filter 213, the second mixer 215 is of the image rejection type. This lessens the image cancellation function of the SAW filter 213. The 10.75 MHz IF signal passes through the band pass filter (BPF) 216, then is mixed with a signal from the local oscillator 218 with the third mixer 217, and further passed through the band pass filter (BPF) 219 to convert it to 1.15 MHz. Then, the signal detected by the limiter 220 is sent to the modem portion 221.

On the other hand, the /4 QPSK modulation wave formed in the /4QPSK modulator 2214 of the modem portion 221 is inputted as digital data to a D/A converter not shown in the drawing. At the D/A converter, it becomes a 10.75 MHz modulation wave, and the unnecessary signals are deleted by the band pass filter (BPF) 222. The 10.75 MHz IF signal is inputted to the transmitting mixer 223, and mixed with a signal from the local oscillator 218 to be converted to 248.45 MHz. This transmitting side IF signal is passed through a SAW filter 213 shared with reception to delete the unwanted signals such as images, then inputted via the transmission-reception switching FET switch 212 and power regulating portion 224 to the transmitting mixer 225. This mixer 225 is mixed with a first local signal from the synthesizer 210, and converted to a transmission frequency. This signal is inputted to a power amp 226 through a band pass filter 206 shared with reception. At this power amp 226, the required power is amplified onto the signal, and the amplified signal has its high frequency part deleted by the low pass filter (LPF) 227, then passed through the transmission switching FET switch 202 to be emitted from the antenna 201.

On the other hand, an audio signal inputted from the microphone 234 is digitized in the PCM codec 228, a PCM signal inputted at 64 Kbps is ADPCM converted (compressed) in the ADPCM codec 2211, and formed into 32 Kbps data. This data is temporarily stored in the buffer 2212, then formed into a TDMA frame with the frame processor 2213. At this time, additional information such as the unique words CI, SA and CRC are added, thus increasing the data rate to 384 Kbps. This data is converted to 10l75 MHz in the /4 QPSK converter 2214 and inputted to a D/A converter which is not shown in the drawing. On the other hand, the received 1.15 MHz data is detected by the /4QPSK demodulator 2215, expanded to 64 Kbps with the ADPCM codec 2211, D/A converted with the PCM codec 228 and outputted to the speaker 233. Aside therefrom, the control of the reception/transmission switching timing, RSSI detection determination, setting of AFC control and synthesizer, and control of the radio system are performed. Additionally, in the case of Embodiment 2, when remote operation data are received, a protection processing portion 2305 for eliminating damage suffered by the owner of the portable electronic device is controlled based on the received remote operation data, thereby performing control to perform a protection process for increasing the security relating to property or information of the owner of the portable electronic device.

Next, the case where the owner of the portable electronic device has lost or had stolen the portable electronic device shall be described. In this case, a protection process control routine for increasing security as shown in Fig. 5 is performed. First, in step S10, the owner of the portable electronic device

inputs remote operation data to initiate communications with respect to the owned portable electronic device using a personal computer 32 through a modulator-demodulator (modem) with respect to the network control station 36. In this case, the content of the remote operation data to be sent is chosen according to the conditions (theft or loss) whereby the portable electronic device is not in possession and the level of importance of the information stored inside. The remote operation data has a control code which the owner has alone added beforehand, and a key word which only the owner knows. Therefore, one other than the owner, for example, the finder will not be able to arbitrarily send or undo the remote operation data with respect to the owner's portable electronic device.

Additionally, if the owner of the portable electronic device does not have a personal computer 32 in the network system of the portable electronic device, or even if owned, the system is not such that the network control station 36 can be activated through a modem, a request is made to the base station 34 of the portable electronic device to transmit remote operation data from a common telephone 31 in a public line network 30. Alternatively, the remote operation data is inputted by a push-button line.

Next, in step S11, the remote operation data inputted by the owner of the portable electronic device is transferred to the base station 34 through a public or dedicated line network 30. In the next step S12, the remote operation data is sent by radio from the base station 34 of the portable electronic device.

As described above, remote operation data inputted from the personal computer 32 is sent through the public or dedicated line network 30 to the base station 34 of the portable electronic device, and sent to the owner's portable electronic device which is not in the possession of the intended owner. If the portable electronic device has a bi-directional dual communication function, it establishes a link and transmits to the personal computer 32 operated by the owner that the reception by the portable electronic device has been reliably performed.

Therefore, in Embodiment 2, as a result of identification of remote operation data received with radio communication means as the transmission medium, damage suffered by the owner of the portable electronic device can be eliminated, enabling security relating to property or information of the owner of the portable electronic device to be increased.

(Embodiment 3)

Next, among the problems which could occur when the portable electronic device of an owner has lost or had stolen the device and another person has found the portable electronic device, there are problems wherein the owner of the portable electronic device may suffer damage such as having private information or important data seen or being forced to pay for communication fees which have not been used, and problems of damage suffered to communication partners or partner information in connection with partners which the owner of the stolen or lost portable electronic device has communicated with, such as transmitting to what was believed to be the owner of the portable electronic device without knowing that the conditions are not appropriate.

Therefore, in Embodiment 3 of the present invention corresponding to claim 3, when the owner of the portable electronic device has lost or had stolen the portable electronic device, the protection process control routine for increasing security which is shown in Fig. 5 is performed. In step S10, the owner of the portable electronic device inputs remote operation data to start communications with the owned portable electronic device using a personal computer 32 through a modem with respect to the network control station 36. In this case, the content of the remote operation data that is sent is chosen according to the conditions (theft or loss) whereby the portable electronic device has fallen out of its rightful hands and the level of importance of information stored inside. A control code has been appended to the remote operation data beforehand, and this control code is a key word known only to the owner.

Thus, in a portable electronic device comprising protection processing means for eliminating damage suffered by the communication partners or partner information transmitted to the owner of the portable

electronic device due to the identification results of remote operation data which have been data received with radio communication means as the transmission medium, protection processing means for preventing damage suffered to the communication partner or partner information confirms that a key word pre-stored in the memory means by the owner of the portable electronic device matches key word information resulting from identification when remote operation data has been received with radio communication means as the medium, after which the protection processes explained in Embodiment 15 to be described below are performed.

That is, due to the remote operation data, at least one of the following are performed:
a. a protection process for transmitting to partners to which transmissions have been made with the portable electronic device predetermined information that the owner is under circumstances of not being able to receive,
b. a protection process for suspending a function of receiving information from partners to which transmission have been made with the portable electronic device,
c. a protection process for transmitting data being communicated or used to partners to which transmissions have been made with the portable electronic device,
d. a protection process for suspending a function of transmitting transmitted information to partners to which transmissions have been made with the portable electronic device,
e. a protection process for transmitting a lost message pre-inputted by the owner and stored in the memory means to partners to which transmissions have been made with the portable electronic device, and
f. a protection process for preventing use of the portable electronic device protecting system to partners to which transmissions have been made with the portable electronic device.

Therefore, in Embodiment 3, for partners who have transmitted to the owner of the lost or stolen portable electronic device, it is possible to know that the portable electronic device of the communication partner is in an inappropriate condition, and to prevent the communication partner or partner information from also suffering damage by means of a protection process.

(Embodiment 4)

When the owner of the portable electronic device has had stolen or lost the portable electronic device, by transmitting a key word and remote operation data for a protection process control routine to increase security as shown in Fig. 5 above to the portable electronic device of the owner which is not in the possession of the owner, the protection processing means of the portable electronic device performs the remote operation data processing routine shown in Fig. 6. Herebelow, the processing routine shall be described with reference to Fig. 6.

In Fig. 6, in step S20, the lost portable electronic device receives the key word and remote operation data, and in the following step S21, identifies whether the key word of the remote operation is the key word pre-stored in the memory means by the owner. Here, if not matched, the protection processing system is terminated and the normal mode is resumed. Additionally, if the key words match, the protection processing system is initiated, and a device protect function is activated. Then, it is determined whether or not it is remote operation data. Here, if not remote operation data, the protection processing system is terminated, and the normal mode is resumed. On the other hand, if remote operation data, then the process advances to step S22 and the remote operation data is analyzed for the type of protection.

The remote operation data has the codes for all protection processes predetermined, so that for example, "issue warning", "display message", "contact owner", "prohibit calling function", "prohibit data output", "delete memory data", "cancel communication line number" and "power off" are separated by predetermined codes and the process advances to the respective protection processing routines.

That is, in step S23, if the content of the remote operation data is found to match the code for "issue warning", the process advances to step S24 and a protection process of "issue warning" is performed. If

there is no match in step S23, the procedure advances to step S25 corresponding to the next processing code, and advances sequentially to the matching codes. The same is true for the other types of remote operation data, so that the corresponding protection process is performed when there is a match. If there are codes that are not applicable, the protection processing system is terminated or fixed protection processes are performed.

Next, in step S25, it is determined whether or not the content of the remote operation data matches with the code "display message", and if there is a match, the procedure advances to step S26 to perform the protection process of "display message". If there is no match in step S25, the procedure advances to step S27 for the next processing code. In step S27, it is determined whether the remote operation data matches with the "prohibit calling function" code, and if there is a match, the procedure advances to step S28 to perform a protection process for "prohibit calling function". If there is no match in step S27, the procedure advances to step S29 for the next processing code.

In step S29, it is determined whether or not the remote operation data matches the code for "contact owner", and if there is a match the procedure advances to step S30 to perform the protection process for "contact owner". If there is no match in step S29, the procedure advances to step S31 for the next processing code.

In step S31, it is determined whether or not the remote operation data matches the code for "delete memory data", and if there is a match the procedure advances to step S32 to perform the protection process for "delete memory data". If there is no match in step S31, the procedure advances to step S33 for the next processing code. In step S33, it is determined whether or not the remote operation data matches the code for "prohibit data output", and if there is a match the procedure advances to step S34 to perform the protection process for "prohibit data output". If there is no match in step S33, the procedure advances to step S35 for the next processing code.

In step S35, it is determined whether or not the remote operation data matches the code for "cancel communication line number", and if there is a match the procedure advances to step S36 to perform the protection process for "cancel communication line number". If there is no match in step S35, the procedure advances to step S37 for the next processing code. In step S37, it is determined whether or not the remote operation data matches the code for "transfer memory data", and if there is a match the procedure advances to step S38 to perform the protection process for "transfer memory data". If there is no match in step S37, the procedure advances to step S39 for the next processing code. In step S39, it is determined whether or not the remote operation data matches the code for "identify user", and if there is a match the procedure advances to step S40 to perform the protection process for "identify user". If there is no match in step S39, the procedure advances to step S41 for the next processing code.

In step S41, it is determined whether or not the remote operation data matches the code for "power off", and if there is a match the procedure advances to step S42 to perform the protection process for "power off". If there is no match in step S41, the procedure advances to step S43 for the next processing code, and if the code does not match any of the codes, then the protection processing system is terminated at step S45. Otherwise, in step S44, a protection process, for example for "power off" is performed as a fixed protection process and the procedure is completed.

In Embodiment 4 as described above, the portable electronic device stores in memory means a key word previously inputted by the owner, and upon receiving remote operation data with radio communication means as the medium, records the protection processing code information from the results of the identification in recording means, and upon confirming a match between the key word in the memory means and protection processing code information, performs the process shown in Fig. 6, thereby achieving protection of the portable electronic device and chooses the optimum protection process on a case-by-case basis to apply the optimum procedure.

(Embodiment 5)

The protection processing (a) of the protection processing means in Embodiment 5 of the present invention shall be described with reference to Fig. 7.

The protection process (a) is a "power off" protection process in which the original functions of the portable electronic device are suspended so that anyone other than the owner of the portable electronic device will not be able to use the lost or stolen portable electronic device.

Fig. 7 is a flow chart showing the "power off" protection process routine for suspending the original functions of the portable electronic device. First, in step S441, it is determined whether the "power off" flag is on, and if the "power off" flag is not on, the procedure advances to step S442, without performing the "power off" protection process. Additionally, when the "power off" flag is on, the procedure advances to step S443 to turn the power on switch disable flag on. Then, in step S444, the power of the portable electronic device is turned forcibly off, the "power off" protection process is performed (step S445), and an instruction to prohibit the power from being turned on is executed with priority.

When a "power off" protection process has been performed with remote operation data in this way, even if the power switch of the portable electronic device is tuned on in manual mode, the control portion confirms in the power on sequence that the flag is on, and forces the power off. Therefore, the power of the portable electronic device will not turn on, so that even if stolen, it cannot be used by others, and line usage fees will not be incurred for invalid use.

This "power off" protection process turns the power switch of the portable electronic device off, and is a procedurally extremely clear protection process, so as to be suited for application as a protection process used as a final measure when the owner has realized that the portable electronic device has been lost or stolen, but cannot perform the procedures for the protection processes (b)-(j). Furthermore, the "power off" can be performed in combination to follow the other protection processes (b)-(j).

Additionally, the "power off" protection process has the purpose of suspending the original functions of the portable electronic device, and includes all hardware means such as means for rebooting the microcomputer or turning the drive oscillator function off among means other than turning the above-described power on switch disable flag on.

By performing at least one of the processes among many protection processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with Embodiment 5, the power cannot be turned on, and the protection process effectively kills the original functions of the device, thus holding the damage to the loser of the device to a minimum.

(Embodiment 6)

The protection process (b) of the protection processing means of Embodiment 6 of the present invention shall be described with reference to Fig. 8.

The protection process (b) is the protection process of "issue warning" wherein a visual or audio alarm is issued and use is prohibited when someone other than the owner of the lost or stolen portable electronic device attempts to use it. It is made more likely to be returned from the finder to the owner, for example, by displaying the address and telephone number or means of contact of the owner on the display portion of the misplaced or lost portable electronic device, and displaying a message to the finder, or be issuing an audio message through the speakers.

Fig. 8 is a flow chart showing the protection process routine for "issue warning" to suspend the original

functions of the portable electronic device. In the protection process routine of "issue warning", first, in step S241, it is determined whether the "issue warning" flag is on, and if the "issue warning" flag is not on, the procedure advances to step S242 without performing the protection process for "issue warning". On the other hand, if the "issue warning" flag is on, the procedure moves to step S243, an alarm is issued from the speakers, and the entire surface of the display portion of liquid crystal or the like is made to blink (step S244). Then, the alarm tone generating time and display portion display time are counted (step S245), and it is determined whether a predetermined period of time has passed (step S246). Here, if the predetermined period of time has not passed, the procedure returns to step S243, and if the predetermined period of time has passed, the procedure returns to step S241.

In this way, even if lost or stolen, others will not be able to stop the alarm or stop the repeatedly blinking display on the display portion. Therefore, when lost, it is easily found by a third party, while also precluding the finder from using it for return to the owner.

However, since repeated alarm tones and blinking of the display portion consume a large amount of the power in the batteries of the portable electronic device, there is the risk of wearing out the batteries without being discovered by a third party, so these are driven for only a fixed period of time.

By performing at least one of the other processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with the present embodiment, the protection process which demands the prohibition of use of the device by others by issuing a warning to the finder of the device prevents use by others aside from the loser of the device, while also making it likely to be returned to the owner.

(Embodiment 7)

The protection process (c) of Embodiment 7 of the present invention shall be described with reference to Fig. 9.

The protection process (c) is a protection process of "display message" wherein the means of contact or a message which have been previously recorded in memory means by the owner are displayed when anyone other than the owner of the lost or stolen portable electronic device attempts to use it, thus enabling the device to be recovered. For example, by displaying the means of contact such as address and telephone number of the owner of the lost or stolen portable electronic device and a message to the finder on the display portion, or issuing a message from the speakers, the finder can be prevented from using it and it can be returned to the owner.

Fig. 9 is a flow chart showing the routine for a "display message" protection process to suspend the original functions of the portable electronic device. First, in step S261, it is determined whether the "display message" flag is on, and if the "display message" flag is not on, the procedure advances to step S262, without performing the protection process of "display message". If the "display message flag is on, the procedure advances to step S263 to select a message by means of the message code number, and displays the predetermined display content 1 which has been stored on the display portion (step S264). Then, a predetermined message 1 which has been stored is issued from the speakers (step S264A), and a protection process of displaying a message is performed (step S267).

Additionally, when a message code number is used to select another message, the predetermined display content 2 which has been stored is displayed on the display portion (step S265). Then, a predetermined message 2 which has been stored is issued from the speakers (step S265A), and the message display protection process is performed (step S267). Additionally, if yet another message has been chosen by means of the message code number, the predetermined display content 3 which has been stored is

displayed on the display portion (step S266). Then, a predetermined message 3 which has been stored is issued from the speakers (step S266A), and a protection process of displaying a message is performed (step S267).

Thus, with the routine for the protection process of "display message", if the message display flag is turned on, a predetermined display content which has been previously stored is displayed on the display portion of liquid crystal or the like, so that if anyone other than the owner of the portable electronic device uses it, a contact address and message which have been previously stored in the memory means by the owner are displayed.

In this case, it is possible to have a plurality of types of "display message" protection processes separated by means of code numbers, so that the messages can be changed according to the location and situation whereby the owner had it lost or stolen, such as by displaying "means of contacting the owner", "address", "telephone number", "request to finder" and "reward to finder". For example, in the case of a "request to finder", a message such as "The finder of this device is asked to contact the following. My name is ___. My telephone number is ___. Thank you." is displayed and issued from the speakers. Alternatively, in the case of a "reward to finder", a message such as "The finder of this device is asked to contact the following. A reward of ___ will be given. The telephone number is ___. The return address is ___." is displayed and issued from the speakers.

Thus, in the present embodiment, the means of contact such as the address and telephone number of the owner of the lost or stolen portable electronic device and a message to the finder is displayed on the display portion, or issued from the speakers, so that if the finder is able to contact the owner, it can be returned to the owner. Additionally, if a return request message is made each time the finder uses the device, it is possible to keep the finder from using it.

By performing at least one of the other processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with the present embodiment, the protection process of asking the finder of the device for return of the device by displaying a message prevents others aside from the loser of the device from using it, and can be effective in prompting its return to the owner.

(Embodiment 8)

The protection process (d) of the protection processing means for Embodiment 8 of the present invention shall be described with reference to Fig. 10.

The protection process (d) is a protection process of "contact owner" wherein the original functions are suspended and only the contact address which has been previously inputted by the owner in the memory means is called when anyone other than the owner of the lost or stolen portable electronic device attempts to use it. For example, if the owner of the lost or stolen portable electronic device has registered the contact address of a security company which has been previously contracted, then if the finder attempts to dial a number without permission, all of the signals will go to the security company.

Fig. 10 is a flow chart showing the protection process routine of "contact owner" for suspending the original functions of the portable electronic device. First, in step S301, it is determined whether the "contact owner" flag is on, and if the "contact owner" flag is not on, the procedure advances to step S302 without performing the protection process for "contact owner". If the "contact owner" flag is on, the procedure goes to step S303, where the preset contact address is selected from the memory means, and a predetermined contact address 1 which has been stored is displayed on the display portion (step S304). Then, the predetermined contact address 1 which has been stored is automatically called and connected

(step S304A), to perform the protection procedure of contacting the owner (step S307).

Additionally, if another contact address is chosen, the predetermined contact address 2 which has been stored is displayed (step S305). Then, the predetermined contact address 2 which has been stored is automatically called and connected (step S305A), and the protection process for contacting the owner is performed (step S307).

Thus, with the routine for the protection process of "contact owner", if the contact owner flag is on, it becomes possible to contact only the predetermined address which has been previously stored. That is, when anyone other than the owner attempts to use the stolen or lost portable electronic device, it is confirmed that the owner contact flag is on, and the device shifts to calling only the predetermined contact address with priority. Therefore, if the owner has pre-registered himself as the contact, it is always possible to communicate with the finder, thus allowing for a request to return the device to be made directly to the finder. Additionally, in this case, the finder cannot communicate with anyone other than the owner, so that even if stolen, a third party will not be able to use it, thus preventing line usage fees from being incurred on invalid use.

By performing at least one of the other processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with the present embodiment, a protection process whereby the finder of the device can be contacted by means of calling the owner when using the device, thus allowing for a request to return the device to be made, preventing use by others and enabling it to be returned to the owner when the device has been lost.

(Embodiment 9)

The protection process (e) for the protection processing means according to Embodiment 9 of the present invention shall be described with reference to Fig. 11.

The protection process (e) is a protection process of "prohibit calling function" for suspending functions pre-inputted by the owner among the original functions of the lost or stolen portable electronic device. Of the original functions of the device, a protection process is performed on only a portion of the functions; for example, calling is prohibited by suspending the dial input function, or only the recording function is suspended for security protection of personal data relating to the owner.

Fig. 11 is a flow chart showing the protection process routine of "prohibit calling function" for suspending the original functions of the portable electronic device. First, in step S281, it is determined whether or not the "prohibit calling function" flag is on, and if the "prohibit calling function" flag is not on, the procedure advances to step S282, without performing the protection process of "prohibit" calling function. Additionally, if the "prohibit calling function" flag is on, the procedure advances to step S283, turns off the calling function which nullifies the call request code number, and performs the protection process of prohibiting the calling function (step S284).

Thus, with the protection process routine of "prohibit calling function", if the prohibit calling function flag is turned on, calls are prohibited. That is, if anyone other than the owner attempts to use the stolen or lost portable electronic device, it is confirmed that the calling function flag is on, and a process for prohibiting calls is performed with priority. Therefore, the finder will not be able to make any calls, so as not to be able to communicate with others, thus preventing a third party from using it in the case of theft, and the owner will not be forced to pay for line usage fees incurred on invalid use.

By performing at least one of the other processes by means of remote operation data, even if the portable

electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with the present embodiment, the protection process of prohibiting the calling function against use by the finder of the device prevents use by others when the device is lost, thereby avoiding fees generated on invalid use.

(Embodiment 10)

The protection process (f) of the protection processing means of Embodiment 10 of the present invention shall be described with reference to Fig. 12.

The protection process (f) is a protection process of "prohibit data output" for prohibiting the output of data from the lost or stolen portable electronic device. For example, personal data or confidential data relating to the owner of the portable electronic device is stored with a specific memory-designated lock, so as not to be able to be opened without using a procedure other than the pre-designated key word.

Fig. 12 is a flow chart showing the routine for the protection process of "prohibit data output" for suspending the original functions of the portable electronic device. First, in step S341, it is determined whether the "prohibit data output" flag is on, and if the "prohibit data output" flag is not on, the procedure advances to step S342, without performing the protection process of "prohibit data output". If the "prohibit data output" flag is on, the procedure advances to step S343, the calling function is chosen to be turned off so as to invalidate the calling request code, and a protection process of prohibiting data output is performed (step S344).

Thus, with the protection process routine of "prohibit data output", the outputting of data is prohibited by turning the prohibit data output flag on. That is, if anyone other than the owner of the lost or stolen portable electronic device attempts to use it, it is confirmed that the prohibit data output flag is on, and a procedure for prohibiting data output is performed with priority. Therefore, the finder or a third party will not be able to output data, so that data or personal information of the owner will not be able to be seen or used by anyone other than the owner. Additionally, a portable electronic device which has been protected by the process of "prohibit data output" after having been stolen or lost becomes nothing more than an inert object to anyone other than the owner, so that the damage suffered by the owner concerns only the hardware of the portable electronic device, thereby increasing the security of information or property of the owner.

By performing at least one of the other processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with the present embodiment, the protection process of prohibiting data output which protects personal data and information in the device prevents use by others aside from the one losing the device, thereby avoiding fees incurred on invalid use.

(Embodiment 11)

The protection process (g) of the protection processing means of Embodiment 11 of the present invention shall be described with reference to Fig. 13.

The protection process (g) is a protection process of "delete memory data" wherein the data in the memory means of the lost or stolen portable electronic device is deleted so as not to be seen or used by others, whereby personal information and data relating to the owner is erased from the memory portion of

the portable electronic device, thereby avoiding disclosure to others.

Fig. 13 is a flow chart showing the protection process routine of "delete memory data" for suspending the original functions of the portable electronic device. First, in step S321, it is determined whether the "delete memory data" flag is on, and if the "delete memory data" flag is not on, the procedure advances to step S322 without performing the protection process of "delete memory data". Additionally, if the "delete memory data" flag is on, the procedure advances to step S323, the predetermined area in the memory means is erased, and the selection of data (personal information, specific information of the device and call numbers) in the user area of the memory means is prohibited. Thereafter, the protection process of deleting the memory data is performed (step S324).

Thus, with the protection process routine of "delete memory data", the memory data is deleted if the memory data delete flag is turned on. That is, if anyone other than the owner attempts to use the lost or stolen portable electronic device, it is confirmed that the memory data delete flag is on, and a process for deleting the memory data is performed with priority. Therefore, even if the finder or a third party attempts to use the lost or stolen portable electronic device, the data in memory has been erased, thereby making it impossible for anyone other than the owner to view or use personal information or data of the owner. Additionally, a portable electronic device which has been protected by the process of "delete memory data" after having been stolen or lost becomes nothing more than an inert object to anyone other than the owner, so that the damage suffered by the owner concerns only the hardware of the portable electronic device, thereby increasing the security of information or property of the owner.

By performing at least one of the other processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with the present embodiment, the protection process of deleting the memory data protecting personal data or information inside the device prevents others aside form the loser using the device, thereby avoiding fees incurred on invalid use and inhibiting misuse of the personal data and information by others.

(Embodiment 12)

The protection process (h) of the protection processing means according to embodiment 12 of the present invention shall be described with reference to Fig. 14.

The protection process (h) is a protection process of "cancel communication line number" wherein the communication line number of the lost or stolen portable electronic device is canceled so as to make it unusable to others, thereby avoiding communication fees incurred due to misuse by others.

Fig. 14 is a flow chart showing the protection process routine of "cancel communication line number" for suspending the original functions of the portable electronic device. First, in step S361, it is determined whether the "cancel communication line number" flag is on, and if the "cancel communication line number" flag is not on, the procedure advances to step S362 without performing the protection process of "cancel communication line number". If the "cancel communication line number" flag is on, the procedure advances to step S363, and the communication dial switch disable flag is turned on. Then, in step S364, the power of the portable electronic device is turned forcibly off, and the protection process of canceling the communication line number is performed (step S365).

Thus, in the protection process routine of "cancel communication line number", if the cancel communication line number flag is turned on, the communication line number of the portable electronic device is canceled. That is, if anyone other than the owner of the stolen or lost portable electronic device attempts to use it, it is confirmed that the cancel communication line number flag is on, and the

procedure advances to a process for canceling the communication line number stored in the portable electronic device with priority. Therefore, even if the finder or a third party attempts to use the lost or stolen portable electronic device, the communication line number which must be recorded has been canceled, thus making it unusable to others. Additionally, a portable electronic device which has been protected by the process of "cancel communication line number" after having been stolen or lost becomes nothing more than a simple object to anyone other than the owner, so that the damage suffered by the owner concerns only the hardware of the portable electronic device, thereby increasing the security of information or property of the owner. Furthermore, the communication line number can only be inputted by a special method by the manufacturer or vendor of the portable electronic device, so that it is a number specific to each device recorded only once in the internal memory medium portion where registered content is held even if the power is turned off.

By performing at least one of the other processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with the present embodiment, the protection process cancels the communication line number against use by the finder of the device, thus making the calling function impossible to use, thereby preventing use by others aside from the one losing the device, and avoiding fees incurred on invalid use.

(Embodiment 13)

The protection process (i) of the protection processing means of Embodiment 13 of the present invention shall be described with reference to Fig. 15.

The protection process (i) is a protection process of "transfer memory data" wherein the data in the memory means of the lost or stolen portable electronic device is transferred to another predetermined electronic device, so that the personal information and data relating to the owner in the memory portion of the portable electronic device is transferred to another predetermined electronic device, and thereafter, the personal information or data in the memory portion of the device is diverted to the other predetermined electronic device.

Fig. 15 is a flow chart showing the protection process routine of "transfer memory data" for suspending the original functions of the portable electronic device. First, in step S381, it is determined whether the "transfer memory data" flag is on, and if the "transfer memory data" flag is not on, the procedure advances to step S382 without performing the protection process of "transfer memory data". If the "transfer memory data" flag is on, the procedure advances to step S383 where the memory data is read from the memory means, and the memory data is transmitted (step S384). Then, it is determined whether the data transfer has been completed (step S385). Here, if the data transfer has not been completed, the procedure returns to step S383, and if the data transfer has been completed, the procedure advances to step S386, where the memory portion is destroyed and the data erased. Then, the protection process of memory data transfer is performed (step S387).

Thus, in the protection process routine for "transfer memory data", if the transfer memory data flag is on, the memory data is transferred and recovered. As a result, personal information and data recorded in the lost or stolen portable electronic device can be read and transferred, after which a process for erasing the memory data in the memory means of the device is performed with priority. Therefore, by means of the present protection process, when the portable electronic device has been stolen or lost, the owner can read and transfer the memory data to another predetermined electronic device to thereby recover it, then erase the original memory data, so that even if the finder or a third party attempts to use the lost or stolen portable electronic device, the memory data is erased, thus making it impossible for anyone other than the owner to view or use the personal information or data of the owner.

By performing at least one of the other processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

In particular, with the present embodiment, the protection process of "transfer memory data" which transfers the personal data and information inside the device by remote operation enables personal data and information inside to be transferred and recovered before being used by someone aside from the one who has lost the device, after which the memory data inside the device is erased, thereby preventing use by others for the loser of the device, and avoiding fees incurred on invalid use.

(Embodiment 14)

The protection process (j) of the protection processing means according to Embodiment 14 of the present invention shall be described with reference to Fig. 16.

The protection process (i) is a protection process of "identify user" wherein the user is identified, and it is made impossible for anyone other than the owner to use the portable electronic device. The identification of the user is performed, for example by user identification means such as password input, fingerprint recognition or voice recognition, and performs a protection process when anyone other than the owner uses the portable electronic device.

Fig. 16 is a flow chart showing the protection process routine of "identify user" for suspending the original functions of the portable electronic device. First, in step S401, it is determined whether the "identify user" flag is on, and if the "identify user" flag is not on, the procedure advances to step S402, without performing the "identify user" protection process. Additionally, if the "identify user" flag is on, the procedure advances to step S403, where first the calling function of the device is turned off, followed by a determination of whether it is the user identification number (step S404). Here, if not the correct user identification number, the process returns to step S402, and if the correct user identification number, the procedure advances to one of steps S405, step S406 or step S407 to perform identification of the user.

One of the ways to identify the user is to request the input of a password upon use, compare the input password with a password preset and registered by the owner of the portable electronic device (step S405), and determine whether the password has matched (step S405A). Here, if there is a match, the procedure advances to step S409 to enable normal use. Additionally, if there is no match, the number of times for accepting the input of the wrong password is set at three times (step S405B), so that if the wrong password is inputted more than three times, a more powerful protection procedure is performed (step S408). The password preset by the owner at this time is stored just once in a memory portion which holds the registered content even if the power is turned off. While protection processes in which operations are initiated only after a password has been inputted before use have been known conventionally, but it can be bothersome for normal usage and this type of protection process is often normally disengaged. However, the present protection process has the characteristic that when a portable electronic device has been lost or stolen, the owner of the portable electronic device sends remote operation data requesting protection to the portable electronic device, and activates the functions of protection processing by means of a password.

Additionally, as another example of user identification, the user of the portable electronic device is asked to input a fingerprint, and this is compared with a fingerprint which has been previously set and registered by the owner of the portable electronic device (step S406), to determine whether the fingerprints match (step S406A). Here, in order for the user to input the fingerprint, it is possible to add a function of detecting the fingerprint at the portion where the thumb is in contact on the hand holding the portable telephone, and a function of recognizing fingerprints. Accordingly, if the fingerprints match, the procedure advances to step S409 to make normal usage possible. On the other hand, if the fingerprint is found not to match, then the number of trials for inputting of the wrong fingerprint is set at three (step

S406B), and if the wrong fingerprint is inputted three or more time, a more powerful protection process is performed (step S408).

Additionally, as another example of user identification, the password is verbalized, so that the audio data (voiceprint) of the pre-registered password is collated with the voiceprint inputted from the microphone (step S407), to determine whether the voiceprints match (step S407A). Here, if the voiceprints are found to match, the procedure advances to step S409 to enable normal usage. If the voiceprints do not match, then the number of times allowed for the wrong voiceprint to be entered is set at three (step S407B), and if the wrong voiceprint is inputted more than three times, a more powerful protection process is run (step S408).

Thus, with the protection process routine of "identify user", a password, fingerprint or voiceprint is identified by user identification means when the user identification flag is turned on, and if anyone other than the owner is found to be using the portable electronic device, the user identification flag is confirmed to be on, and a process for prohibiting calls from the device is performed with priority. As a result, the finder will not be able to make calls and will not be able to communicate with others.

By performing at least one of the other processes by means of remote operation data, even if the portable electronic device is stolen or lost, the personal data in the portable electronic device is protected, and a predetermined level of security can be gained so as to eliminate damage suffered to the owner due to use by others.

(Embodiment 15)

Next, the protection process of Embodiment 15 corresponding to claim 15 of the present invention shall be described. The protection process according to this embodiment is composed from the following.

The protection process (a) is a protection process of transmitting predetermined information that the owner is not in a receptive condition to the partners who transmit to the portable electronic device, so that by notifying the transmitting partners that the owner is not in a situation such as to be able to receive personal information or data, its transmission is avoided before it happens, thereby protecting personal information or data from leaking to other people such as the finder.

The protection process (b) is a protection process wherein the function of receiving information received from those who have transmitted to the portable terminal device is suspended, suspending the function of receiving information received from partners so that personal information and data is not leaked to other people such as the finder.

The protection process (c) is a protection process of transmitting to those who have transmitted to the portable electronic device data indicating that the line is busy or being used, so as to spontaneously send signal data to the effect that the line is busy or being used to transmitting partners before they send personal information or data to the owner, thereby protecting against leakage of personal information and data to others such as the finder.

The protection process (d) is a protection process for suspending the function of transmitting information to those transmitting to the portable electronic device, so that the function of transmitting information is suspended during the performance of communication procedures before those who are transmitting transmit personal information or data to the owner, such as by not transmitting an access signal, thereby avoiding communications.

The protection process (e) is a protection process of transmitting a loss message pre-inputted and stored in the memory means by the owner for those transmitting to the portable electronic device, and is such as to replace the signal data that the line is busy or being used in the protection process (c) with the loss message pre-inputted and stored in the memory means and to send this spontaneously, so as to avoid

transmission before it happens, thereby protecting personal information and data from leakage to others such as the finder.

The protection process (f) is a protection process of preventing use of the portable electronic device to those transmitting to the portable electronic device, wherein the transfer destinations are fixed and any stored addresses are erased to avoid disclosure to others in order to avoid the problems due to those communicating personal information or data using the portable electronic device found by another person who has found the device as personal information or data of the owner.

As a result of performing at least one of the above protection processes, even if the portable terminal device is, for example, stolen or lost, those transmitting to the owner of the device can be protected of the personal information or data in the portable electronic device, and it is possible to increase a predetermined level of security by eliminating damage suffered by the owner due to use by others.

(Embodiment 16)

Next, a protection process of Embodiment 16 corresponding to claim 16 of the present invention shall be described. This embodiment is such that when radio communication means are taken as the transmission medium to receive a key word signal which the owner has pre-inputted and stored in the memory means, the identification of the remote operation data results in the protection functions of the portable electronic device being forcibly activated, thus providing protection processing means for increasing to a predetermined level of security by eliminating damage suffered by the owner.

In Fig. 1, the owner of the lost or stolen portable electronic device 1 operates a telephone 3 such as a PHS as a portable telephone or a common public telephone to call the portable electronic device 1. In this case, remote operation data of the portable electronic device 1 requiring protection is sent through a public line network 2c from a common public telephone 3A inside or outside a metropolitan area, or through a radio communication line 2b from a PHS 3 as a portable telephone or a PHS data communication terminal.

Next, the protection process of the present embodiment shall be described using the routine for confirming protection shown in Fig. 17.

In many cases, a stolen or lost portable electronic device 1 has been found by another, and communication is possible. Next, the owner who has lost or had stolen the portable electronic device 1 sends a key word signal which the owner has previously inputted and stored in the memory means. When the key word signal stored in the memory means is received, the portable electronic device 1 receives remote operation data at a receiving portion 11 for receiving (step S171), and determines at the identifying portion 12 whether the received remote operation data matches the predetermined key word signal which has been previously stored (step S172). Only if as a result of the identification of the identifying portion 12, a match has been confirmed, a protection confirmation signal is issued (step S173). Due to this protection confirmation signal, the other functions are turned forcibly off (step S174), after which the protecting portion 13 forcibly activates the protection functions of the portable electronic device (step S175), thereby activating a predetermined protection process to eliminate damage suffered by the owner of the portable electronic device.

In particular, with the present embodiment, a key word signal which has been pre-inputted and stored in the memory means by the loser of the device is transmitted to forcibly activate a protection function of the portable electronic device, thereby preventing use of the device by others aside from the one who lost the device.

(Embodiment 17)

Next, Embodiment 17 corresponding to claim 17 will be described with reference to Fig. 18. This

embodiment is provided with protection processing means for increasing a predetermined level of security to eliminate damage suffered by the owner such that when the owner receives a pattern of callup signals pre-inputted and stored in memory means by the owner, as a result of identification of the remote operation data, the portable electronic device is forcibly connected.

That is, the number of callup signals in the first reception are counted (step S101), and it is determined whether this count value can be determined to be the preset number of calls (step S182). Here, if the determination is negative, the procedure returns to step S181, and if affirmative, the procedure advances to step S183. In step S183, the number of callup signals for the second time are counted, and it is determined whether this count value can be considered to be the number of calls preset for the second time (step S184). Here, if the determination is negative, the procedure returns to step S181, and if affirmative, the procedure advances to step S185.

At step S185, the number of callup signals received for the third time are counted, and it is determined whether the count value for the number of calls for the third time can be considered to be the preset number (step S186). Here, if the determination is negative, the procedure returns to step S181, and if affirmative, the procedure advances to step S187. In step S187, the protection system is initiated, and from the callup signal number for the next reception, it is determined whether the content of protection can be recognized (step S188). If protection content is recognized, then the procedure advances to step S189, where the protection content of the remote operation data is analyzed. Then, a protection procedure in accordance with the results of the identification of the remote operation data is performed (step S190).

Thus, even when the person who has found the lost or stolen portable electronic device answers or is not able to communicate, if a pattern of callup signal counts previously inputted and stored in the memory means is received, the recognition of remote operation data results in the operation of applying a predetermined protection process such as by forcibly cutting off the power supply or immediately freezing.

The above-mentioned pattern of callup signal counts if such as to take the line off the hook after 10 callup signals for the first time, take the line off the hook after 5 callup signals for the second time and take the line off the hook after 8 callup signals for the third time, such that if this callup signal count pattern is received as a repeated pattern in a predetermined span of time, then the content of a predetermined protection process is applied.

Claim 8 of the present invention is such that in the remote operation data processing routine of the portable electronic device in Embodiment 4, the method for identifying whether or not there is a remote operation corresponding to the key word operation in step S20 and step S21 of Fig. 6 has been replaced. As a result, the content of each protection process is the same as described above, and their description shall therefore be omitted.

The protection process according to the present embodiment is a practical example of application of a portable electronic device as a portable information terminal telephone device, but it is also applicable to common portable information terminal devices, PHS and cordless telephones.

In particular, with the present embodiment, even if the finder of the device does not answer or is in such as condition as not to be capable of communicating, the remote operation process can be activated by means of a pattern of callup signal counts, thereby preventing others aside from the one losing the device from using it.

(Embodiment 18)

Next, a portable electronic device protecting system of Embodiment 18 corresponding to claim 18 of the present invention shall be described with reference to Fig. 19.

This embodiment offers a portable electronic device protecting system for preventing loss or misplacement of the portable electronic device. In particular, it relates to portable electronic devices having sub devices using weak radio waves or ultrasonic waves, and as in Embodiment 1, the number of cases of loss of this type of portable electronic device everywhere and anytime is increasing, so as to be exceptionally convenient for their compactness and portability but easily stolen. There are no measures that can be taken against loss thereof aside from the owner paying careful attention, but many have experienced just how ineffective a method this is.

As means for resolving these problems, the present embodiment comprises a sub-device comprising oscillating means for prompting a protection process in the portable electronic device, and low-power transmitting means for transmitting an oscillation signal of said oscillating means, and a portable electronic device (main device) comprising low-power receiving means for receiving oscillation data for prompting protection processes from said sub-device, identifying means for identifying operation data received by said low-power receiving means and predetermined protection means for eliminating damage suffered by the owner of the portable electronic device by means of identification results of said identifying means, thereby increasing the security relating to the property or information of the owner of the portable electronic device, wherein the above-mentioned sub device having low power transmitting means should preferably be of a compact lightweight type which can be easily carried like a pendant on a chain or an earring. The sub device can be applied to a hook or belt so as to be inserted securely inside a pocket in clothing or the like, or contained in an earring or pendant to prevent loss of the sub device itself.

The portable electronic device of the main device has receiving means for receiving oscillation data for prompting a protection process from the sub device, and activates predetermined protection means by means of means for identifying the received operation data. Additionally, the distance over which the signal sent by the low power transmitting means is set, for example, to a few meters or so, such that when the above-mentioned transmitting-receiving means is separated, that is, when the main device and sub device are separated by more than a communicable distance, the received signal level becomes less than a predetermined value, whereupon the means for identifying the operation data which has been received recognizes that the portable electronic device of the main device has been separated from the owner by more than the predetermined distance, and therefore that the owner has misplaced or lost the portable electronic device of the main device. Then, predetermined protecting means for eliminating damage suffered by the owner of the portable electronic device is activated as a result of the recognition. The protecting means can, for example, issue a warning buzzer as a warning to make the owner realize what is happening, or activate various protection functions such as in the above-described Embodiment 1 for prompting a protection process in the portable electronic device main device.

Fig. 19 is a structural diagram showing an example of Embodiment 18. In the drawing, the output signal from the oscillator 21 in the sub device is modulated and amplified by the transmitting portion 22, and a predetermined low power signal is sent from the low power transmitting means 23 through the antenna.

On the other hand, the signal is then received from the antenna in the main device by the low power receiving portion 24. The received signal is demodulated and amplified in the transmitting portion 25, and after being detected by the detecting portion 26, it is determined whether the reception level is les than a preset level in the determining portion 27, and it is determined whether or not the spatial distance between the sub device and main device is more than the predetermined distance by means of the reception level. When the spatial distance between the sub device and main device becomes greater than the predetermined distance, the protection means 28 for activating various protection processes to prompt a protection process in the main device is activated, for example, by issuing a warning buzzer to make the owner realize what is happening.

As described above, when the owner is about to lose or misplace the portable electronic device, the present system is activated so as to prevent and avoid loss or misplacement before it happens. Additionally, even when the owner has already lost or misplaced the portable electronic device, various

protection functions for prompting a protection process are automatically activated in the main device, so that even if another person finds it, the security relating to property or information of the owner of the device can be easily increased.

(Embodiment 19)

Fig. 20 is a functional block diagram showing the structure of Embodiment 19 corresponding to claim 19 of the present invention. In the drawing, the sub device comprises an oscillator 41, a transmitting portion 42 for modulating and amplifying an output signal from the oscillator 41, low power transmitting means 43 for sending signals form the transmitting portion 42 to the main device and receiving signals from the main device, a transmitting portion 44 for demodulating and amplifying received signals from the low power transmitting means 43, a detecting portion 45 for detecting demodulated signals, a determining portion 46 for discriminating whether or not the reception level of the detected signal is less than a preset level and discriminating from the reception level whether or not the spatial distance between the sub device and main device is more than a predetermined distance, protecting means 47 for performing various protection processes for protecting the sub device and a resetting portion 48 for resetting the exchange of signals.

Additionally, the main device comprises low power transmitting means 49 for receiving signals from the sub device and sending signals to the sub device, a transmitting portion 50 for demodulating and amplifying signals received by the low power transmitting means 49, a detecting portion 51 for detecting demodulated signals, a determining portion 52 for discriminating whether or not the reception level of detected signals is less than a preset level and determining from the reception level whether or not the spatial distance between the sub device and main device is more than a predetermined distance, protection means 53 for performing various protection processes to protect the main device, a resetting portion for resetting the exchange of signals, an oscillator 55 and a transmitting portion 56 for demodulating and amplifying output signals from the oscillator 55 and outputting them to the low power transmitting means 49.

With this structure, if as shown in Fig. 19, the distance between the main device and sub device of the portable electronic device becomes such as to be incommunicable due to being separated, for example, by a few meters, the received signal level goes below the predetermined value, so that the determining portions 46 and 52 which identify the received operation data find that the portable electronic device of the main device has been separated from the owner by at least a predetermined distance, that is, that the owner has had stolen, misplaced or lost the portable electronic device of the main device, and as a result of this determination, an operation is begun in predetermined protection means 47 and 53 to eliminate damage suffered by the owner of the portable electronic device, thereby to prevent and avoid theft, loss or misplacement before it happens. The protection means 47 and 53, for example, sound a warning buzzer on one or both of the main device and sub device to warn the owner as to what is happening, or activate various protection functions as in the above-described embodiments to prompt protection processes in the portable electronic device main device.

Thus, due to the main device and sub device having means for generating a warning, when the owner is about to have stolen or lose or misplace the portable electronic device, the protection means of the present system is activated to prevent and avoid theft, loss or misplacement before it happens. In particular, when encountering theft and purloining, considering the effect and danger of issuing a warning tone, loss or misplacement can be avoided without being noticed by surrounding people by notifying the owner by means of vibrations instead of generating a warning tone from the sub device. Additionally, it is possible to switch between whether to generate a warning tone to make surrounding people notice, or to resolve the matter without drawing the attention of people close by.

Furthermore, in a portable electronic device wherein the sub device is provided with a function of converting the received signal level to display the distance between the main device and sub device, when the owner is about to lose or misplace the portable electronic device, it is possible to search for the

location of the main device by means of the sub device which displays the distance between the main device and sub device. For example, if the main device is lost to sight indoors, the location of the main device can be figured out from the changes in the display of the distance between the sub device and main device.

Additionally, in the above embodiment, adding a reset portion for resetting the exchange of signals is convenient in practice. Adding a resetting portion has an extremely large effect on the redeployment of the functions of the present embodiment after it has been activated when the owner of the portable electronic device has been on the verge of losing or misplacing it.

Due to what has been described above, a portable electronic device protecting system for preventing loss of misplacement of a portable electronic device as in the present invention can be readily achieved, thus having a considerable effect for preventing loss or misplacement of the portable electronic device.

While the above embodiments describe cases in which the protection process is applied to a portable electronic device as a portable information terminal telephone device, but it can be applied to normal portable information terminals, PHS or cordless telephones.

Effects of the Invention

As is clear form the above examples, the portable electronic device protecting system of the present invention as described above is capable of achieving the following effects.

Due to remote operation by the owner against theft or loss of the portable electronic device (data processing device having radio signal communicating means including PHS and cellular telephones), predetermined protection means for eliminating damage suffered by the owner of the portable electronic device is activated, thus increasing the security relating to property or information of the owner of the portable electronic device. That is, the data inside the portable electronic device can be easily protected, and problems such as having to pay fees for use by others can also be avoided.

Additionally, due to the owner actively requesting protection upon the owner realizing that the portable electronic device has been lost or stolen, it is possible to prevent causes of problems to the owner of the portable electronic device. That Is, the content of the memory and specifications of the portable electronic device can be locked for protection.

Additionally, it is also possible for partners with whom the owner of the lost or stolen portable electronic device has communicated to avoid problems such as transmitting to the owner of the portable electronic device without knowing that the conditions are inappropriate, thus causing damage to be suffered by the transmission partner or the partner's information. That is, damage suffered by the owner of a portable electronic device which has been lost or stolen or to the communication partners thereof can be eliminated.

Additionally, according to the portable electronic device protecting system of the present invention, when the owner is about to lose of misplace the portable electronic device, it is possible to prevent and avoid loss or misplacement before it happens due to activation of the main system, as well as to automatically activate various protection functions prompting protection procedures in the main device even when the owner has lost or misplaced the portable electronic device, thereby enabling the security relating to property or information of the owner of the device to be readily achieved even when found by another.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 A schematic structural diagram of a portable electronic device protecting system according to Embodiment 1 of the present invention.

Fig. 2 A functional block diagram showing the structure of a portable electronic device protecting system according to Embodiment 2 of the present invention.

Fig. 3 A hardware structural diagram of the protocol according to Embodiment 2 of the present invention.

Fig. 4 A diagram showing the network system of a portable electronic device according to the present invention.

Fig. 5 A control routine diagram of a protection process for increasing security in the present invention.

Fig. 6 A process routine diagram of remote operation data according to the present invention.

Fig. 7 A flow chart showing a protection process routine for turning the power off according to the present invention.

Fig. 8 A flow chart showing a protection process routine for issuing a warning according to the present invention.

Fig. 9 A flow chart showing a protection process routine for displaying a message according to the present invention.

Fig. 10 A flow chart showing a protection process routine for contacting the owner according to the present invention.

Fig. 11 A flow chart showing a protection process routine for prohibiting a transmission function according to the present invention.

Fig. 12 A flow chart showing a protection process routine for prohibiting data output according to the present invention.

Fig. 13 A flow chart showing a protection process routine for deleting output data according to the present invention.

Fig. 14 A flow char showing a protection process routine for canceling a communication line number according to the present invention.

Fig. 15 A flow chart showing a protection process routine for transferring memory data according to the present invention.

Fig. 16 A flow chart showing a protection process routine for identifying the user according to the present invention.

Fig. 17 A flow chart showing the routine for protection confirmation according to the present invention.

Fig. 18 A flow chart showing a routine for a remote operation process due to a callup signal according to the present invention.

Fig. 19 A structural diagram showing a portable electronic device protecting system according to Embodiment 18 of the present invention.

Fig. 20 A structural diagram showing a portable electronic device protecting system according to Embodiment 19 of the present invention.

Description of Reference Numbers

1	portable electronic device
2a, 2b, 2c	radio signal communicating means
3	telephone (PHS)
3A	telephone
4	relay base station
11	receiving portion (receiving means)
12	identifying portion (identifying means)
13	protecting portion (protecting means)
21	oscillator
22	transmitting portion
23	low power transmitting portion
24	low power receiving portion
25	transmitting portion
26	detecting portion
27	determining portion
28	protecting means
30	public and dedicated line network
31	common telephone
32	personal computer with modulator-demodulator
33	base station
34	base station
35	base station
36	network control station
41	oscillator
42	transmitting portion
43	low power transmitting means
44	transmitting portion
45	detecting portion
46	determining portion
47	protecting means
48	resetting portion
49	low power receiving portion
50	transmitting portion
51	detecting portion
52	determining portion
53	protecting means
54	resetting portion
55	oscillator
56	transmitting portion